Guia do HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools)

Business Desktops HP Compaq

© Copyright 2006 Hewlett-Packard Development Company, L.P. As informações contidas neste documento estão sujeitas à alterações sem aviso.

Microsoft e Windows são marcar registradas da Microsoft Corporation nos Estados Unidos e outros países.

Intel e SpeedStep são marcas registradas da Intel Corporation nos Estados Unidos e em outros países.

As únicas garantias para produtos e serviços da HP são as estabelecidas nas declarações de garantia expressa que acompanham tais produtos e serviços. Nenhuma parte deste documento pode ser inferida como constituindo uma garantia adicional. A HP não será responsável por erros técnicos ou editoriais ou por omissões aqui contidas.

Este documento contém informações de propriedade da HP protegidas por direitos autorais. Nenhuma parte deste documento pode ser fotocopiada, reproduzida ou traduzida para qualquer outro idioma sem a permissão prévia e por escrito da Hewlett-Packard Company.

Guia do HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools)

Business Desktops HP Compaq

Primeira edição: agosto de 2006

Número de peça: 431330-201

Sobre este guia

Este guia fornece instruções para a configuração e uso do gerenciador de segurança HP ProtectTools.

AVISO! O texto apresentado dessa maneira indica que a não-observância das orientações poderá resultar em lesões corporais ou morte.

CUIDADO O texto apresentado dessa maneira indica que a não-observância das orientações poderá resultar em danos ao equipamento ou perda de informações.

Nota O texto apresentado dessa maneira oferece informação adicional importante.

Conteúdo

1 Introdução

HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools)

O software ProtecTools Security Manager oferece os recursos de segurança que são projetados para ajudar na proteção contra acesso não autorizado ao computador, redes e dados críticos. A funcionalidade de segurança avançada é oferecida pelos seguintes módulos:

- Configuração do BIOS HP para ProtectTools
- HP Embedded Security para ProtectTools
- HP Credential Manager para ProtectTools
- HP Java Card Security para ProtectTools

Os módulos disponíveis para seu computador podem variar dependendo do modelo. Os módulos ProtectTools podem vir pré-instalados, fornecidos em CD enviado com o computador, ou disponíveis para compra no Web site da HP. Para obter mais informações, visite http://www.hp.com.

Nota Consulte as telas de ajuda do ProtectTools para instruções específicas sobre os módulos ProtectTools.

Para utilizar o TMP (Trusted Platform Module – ou módulo Trusted Platform), as plataformas que contêm o TPM exigem ambos TCG Software Stack (TTS) e software . Alguns modelos oferecem TSS; se o TSS não for oferecido, poderá ser adquirido junto à HP. Além disso, requer a compra separada de software habilitador de TPM para alguns modelos. Consulte Soluções de terceiros para obter mais detalhes.

Acesso ao HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools)

Para acessar o gerenciador de segurança ProtectTools a partir do painel de controle do Microsoft Windows:

- No Windows XP: Clique em **Iniciar** > **Painel de controle** > **Centro de segurança** > **HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools)**.
- No Windows 2000: Clique em **Iniciar** > **Todos os programas** > **HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools)**.

Nota Depois de configurar o módulo , também é possível acessá-lo a partir da tela de login do Windows. Consulte o HP Credential Manager para ProtectTools para obter mais informações.

Entendendo as funções de segurança

Ao administrar a segurança do computador (particularmente para grandes organizações) uma prática importante é dividir as responsabilidades e direitos entre vários tipos de administradores e usuários.

Nota Em uma organização pequena, ou para uso individual, estas funções podem ser executadas pela mesma pessoa.

No ProtectTools, as tarefas de segurança e privilégios podem ser divididos nas seguintes funções:

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

  Nota Muitos dos recursos no ProtectTools podem ser personalizados pelo diretor de segurança em cooperação com a HP. Para obter mais informações, visite http://www.hp.com.

- Administrador de TI – aplica e gerencia os recursos de segurança definidos pelo diretor de segurança. Também pode ativar e desativar alguns recursos. Por exemplo, se o diretor de segurança decidiu empregar Java Cards, o administrador de TI pode ativar o modo de segurança do BIOS por Java Cards.

- Usuário - utiliza os recursos de segurança Por exemplo, se o diretor de segurança e o administrador de TI decidiram empregar Java Cards no sistema, o usuário pode definir o PIN para o Java Card e utilizar o cartão para autenticação.

Os administradores são encorajados a realizar as “melhores práticas” em restringir os privilégios de usuários-finais e acesso restritivo aos usuários.

Gerenciamento de senhas do ProtectTools

A maioria dos recursos do HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools) são protegidos por senhas. A tabela a seguir relaciona as senhas utilizadas com mais freqüência, o módulo de software onde a senha é definida e a função da senha.

As senhas que forem definidas e utilizadas por administradores de TI apenas também são indicadas nesta tabela. Todas as demais senhas podem ser definidas por usuários regulares ou administradores.

Tabela 1-1 Gerenciamento de senhas

Senha do ProtectTools	Definida neste módulo do ProtectTools	Função
Senha de administrador do utilitário de configuração **Nota** Também conhecida como senha do administrador do BIOS, senha do utilitário de configuração F10 ou senha de configuração de segurança	Configuração do BIOS, pelo administrador de TI.	Protege o acesso ao utilitário de configuração do BIOS do computador e configurações de segurança.
Senha de ativação	Configuração do BIOS	O suporte à autenticação na ativação do HP ProtectTools é uma ferramenta de segurança com base em TPM criada para impedir o acesso não autorizado ao

Tabela 1-1 Gerenciamento de senhas (continuação)

		computador durante sua ativação. O suporte à autenticação na ativação utiliza a senha básica de usuário do HP ProtectTools Embedded Security Uma vez ativada a autenticação na ativação no utilitário de configuração do computador, a senha é definida quando a primeira/próxima chave de usuário básico do Embedded Security é inicializada. O Chip TPM Embedded Security protege a senha de autenticação na ativação.
Senha de administrador de Java Card **Nota** Também conhecida como senha do cartão do administrador do BIOS	, pelo administrador de TI	Vincula o Java Card ao computador para fins de identificação. Permite que um administrador do computador ative ou desative senhas do utilitário de configuração do computador, gerar um novo cartão de administrador e criar arquivos de recuperação para restaurar cartões de usuário ou de administrador.
PIN do Java Card PIN		Protege o acesso ao conteúdo do Java Card e ao acesso ao computador quando um Java Card opcional e um leitor são utilizados. Verifique para ver se a senha de usuário do Java Card está duplicada no PIN; ela é utilizada para registrar a autenticação Java Card.
Senha do arquivo de recuperação Java Card (se disponível)		Protege o acesso ao arquivo de recuperação que contém as senhas do BIOS.
Senha de usuário de Java Card (se disponível) **Nota** Também conhecida como senha do cartão do usuário do BIOS		Vincula o Java Card ao computador para fins de identificação. Permite a um usuário criar um arquivo de recuperação para restaurar um cartão de usuário.
Senha de usuário básico **Nota** Também conhecida como: Senha do Embedded Security, senha de pré-inicialização TPM		Utilizada para acessar os recursos Embedded Security como e-mail seguro, critptografia de arquivo e pasta. Quando ativada como senha de suporte à autenticação na ativação do BIOS, protege o acesso ao conteúdo computador quando é ligado, reiniciado ou restaurado do estado em espera. Também é utilizada para autenticar PSD (Personal Secure Drive) e para registrar a autenticação TPM.
Senha de token de recuperação de emergência **Nota** Também conhecida como: Chave de token de recuperação de emergência	Embedded Security, pelo administrador de TI	Protege o acesso ao Token de recuperação de emergência, que é um arquivo de backup do chip de segurança integrado TPM.
Senha do proprietário.	Embedded Security, pelo administrador de TI	Protege o sistema e o chip TPM contra o acesso não autorizado a todas as

Tabela 1-1 Gerenciamento de senhas (continuação)

		funções de proprietário do Embedded Security
Senha de login do Credential Manager	Credential Manager	Esta senha oferece 2 opções: • Ela pode ser utilizada em vez do processo de login do Windows, permitindo o acesso ao Windows ao Credential Manager simultaneamente. • Ela pode ser utilizada em vez do processo de login individual para acessar o Credential Manager, após fazer o login no Windows.
Senha do arquivo de recuperação do Credential Manager	Credential Manager, pelo administrador de TI	Protege o acesso ao arquivo de recuperação do Credential Manager.
Senha de login do Windows	Painel de controle do Windows	Pode ser utilizado no login manual ou utilizado no Java Card.
Senha de programador de backup **Nota** Uma senha de usuário do Windows é utilizada para configurar o programador de backup de .	Embedded Security, pelo administrador de TI	Define o programador de backup de embedded security
Senha de importação PKCS #12 **Nota** Cada certificado importado possui uma senha específica.	Embedded Security, pelo administrador de TI	A senha utilizada para a chave de criptografia de outros certificados, se importados **Nota** Não é necessária para a operação normal do software; o usuário pode optar por definir esta senha ao utilizar a embedded security para enviar certificados importantes.
Token de restauração de senha	Embedded Security, pelo administrador de TI	Ferramenta para o cliente que permite ao proprietário restaurar a senha de usuário básico, em caso de perda; a senha é utilizada para realizar esta operação de restauração.
Senha de administrador do agente de recuperação Microsoft **Nota** O agente de recuperação pode ser qualquer administrador da máquina local. Se o agente de recuperação for criado, então seria preciso acessar como administrador e uma senha será necessária. O agente de recuperação pode decodificar os dados codificados de todos os usuários, basta abri-lo (não requer o assistente).	Microsoft, pelo administrador de segurança de TI	Assegura para que os dados codificados do Personal Secure Drive (PSD) possam ser recuperados. Consulte http://www.microsoft.com/technet/prodtechnol/winxppro/support/dataprot.mspx para obter mais informações. **Nota** Não é necessária para a operação normal do software; o usuário pode optar por definir esta senha ao utilizar a embedded security para enviar certificados importantes.

Tabela 1-1 Gerenciamento de senhas (continuação)

PIN para Virtual Token Master	Credential Manager	Opção do cliente para armazenar credenciais do proprietário com o Credential Manager
PIN de usuário para token virtual	Credential Manager	Opção do cliente para armazenar credenciais do proprietário com o Credential Manager
Senha do assistente de backup de identidade	Credential Manager, pelo administrador de TI	Utilizado para proteger o acesso a um backup de identidade ao utilizar o Credential Manager
Senha de autenticação por token virtual	Credential Manager	Utilizado para registrar a autenticação de token virtual pelo Credential Manager
Alias de autenticação TPM	Credential Manager	Utilizado em vez da senha de usuário básico pelo gerenciador de credencias, na opção de administrador ou usuário
Login por impressão digital	Credential Manager	O Credential Manager permite ao usuário substituir a senha de login do Windows por um login por impressão digital conveniente e seguro. Diferente da senha, as credenciais de impressão digital não podem ser compartilhadas, doadas, roubadas ou adivinhadas. Utilizada pelo Credential Manager
Autenticação por token USB	Credential Manager	Utilizado pelo Credential Manager como autenticação por token em vez de senha

Logo do Credential Manager com autenticação multifator

O Login do Credential Manager permite que a tecnologia de autenticação multifator para acessar o sistema operacional Windows. Isso intensifica a segurança do login por senha padrão do Windows ao exigir uma autenticação multifator sólida. Também aumenta a conveniência da experiência de login diária, eliminando a necessidade do usuário em lembrar senhas. Um recurso exclusivo do Credential Manager é sua habilidade para agregar diversas credenciais de conta em uma identidade de usuário, que possibilita o uso da autenticação multifator apenas uma vez e acesso múltiplo a diferentes contas do Windows com o mesmo conjunto de credenciais.

A autenticação multifator admite qualquer combinação de senhas de usuário, senhas dinâmicas ou de utilização única, TPM, Java cards, tokens USB, tokens virtuais e biometria. O Credential Manager também admite métodos alternativos de autenticação, que oferecem a possibilidade de múltiplos privilégios de acesso a usuários para um mesmo aplicativo ou serviço. Um usuário pode consolidar todas as credenciais, senha de aplicativo e contas de rede em uma única unidade de dados chamada identidade de usuário. A identidade de usuário é sempre criptografada e protegida com a autenticação multifator.

Criação de uma senha segura

Ao criar senhas, você deve primeiro seguir as especificações que são definidas pelo programa. Em geral, considere as seguintes diretrizes que podem ajudar a criar senhas fortes e reduzir as chances de comprometer sua senha:

- Usar senhas com mais de 6 caracteres, preferencialmente mais de 8.
- Misture as letras na senha.

- Sempre que possível, misture caracteres e inclua caracteres especiais e marcas de pontuação.
- Substitua os caracteres especiais ou números por letras em uma palavra chave. Por exemplo, utilizar o número 1 para letras I ou L.
- Combina palavras de 2 ou mais idiomas.
- Divide uma palavra ou frase com números ou caracteres especiais no meio, por exemplo, “Mary22Cat45”.
- Não utilize uma senha que possa constar em um dicionário.
- Não utilize seu nome para a senha ou outra informação pessoal como data de nascimento, nome de animais de estimação, nome da mãe, mesmo escrito ao contrário.
- Mude as senhas com freqüência. Você pode mudar apenas alguns caracteres que incrementam.
- Se anotar sua senha, não a guarde em um local visível muito próximo ao computador.
- Não salve a senha em arquivo, como em um e-mail no computador.
- Não compartilhe contas ou senhas com ninguém.

Tarefas avançadas

Gerenciamento de configurações do ProtectTools

Alguns dos recursos no ProtectTools Security Manager podem ser personalizados na configuração do BIOS.

Ativar e desativar o suporte para autenticação por Java Card na ativação.

Se esta opção estiver disponível, quando ativada, permite utilizar o Java Card para autenticação de usuário ao ligar o computador.

Nota Para ativar completamente o recurso de autenticação na ativação, é preciso também configurar o Java Card utilizando o módulo Java Card Security para ProtectTools.

Para ativar o suporte para autenticação por Java Card na ativação:

1. Selecione **Iniciar** > **Todos os programas** >**HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools)**.
2. No painel esquerdo, selecione **Configuração do BIOS**.
3. Ao ser solicitada a senha de administrador do BIOS no utilitário de configuração do computador, digite sua senha de administrador e em seguida, clique em **OK**.
4. No painel esquerdo, selecione **Segurança**.
5. Em **Java Card Security**, selecione **Ativar**.

   Nota Para desativar o suporte para autenticação por Java Card na ativação, selecione **Desativar**.

6. Clique em **Aplicar**, depois clique em **OK** na janela **ProtectTools** para salvar suas alterações.

Ativar e Desativar o o suporte para autenticação por Java Card na ativação.

Se esta opção estiver disponível, quando ativada, permite utilizar o chip de segurança integrado TPM para autenticação de usuário ao ligar o computador.

Nota Para ativar completamente o recurso de autenticação na ativação, é preciso configurar o chip de segurança integrado utilizando o módulo Embedded Security for ProtecTools.

Para ativar o suporte para autenticação na ativação para a embedded security:

1. Selecione **Iniciar** > **Todos os programas** > **HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools)**.
2. No painel esquerdo, selecione **Configuração do BIOS**.
3. Ao ser solicitada a senha de administrador do BIOS no utilitário de configuração do computador, digite sua senha de administrador e em seguida, clique em **OK**.
4. No painel esquerdo, selecione **Segurança**.
5. Em **Embedded Security**, selecione **Ativar o suporte à autenticação na ativação**.

Nota Para desativar o suporte para autenticação na ativação para a segurança integarda, selecione **Desativar**.

6. Clique em **Aplicar**, depois clique em **OK** na janela **ProtectTools** para salvar suas alterações.

Gerenciamento de senhas do utilitário de configuração

Você pode utilizar a configuração do BIOS para definir e alterar as senhas de ativação e configuração no utilitário de configuração e também para gerenciar diversas configurações de senha.

CUIDADO As senhas definidas em **Opções de Senha** na Configuração do BIOS são imediatamente salvas, clicando no botão **Aplicar** ou **OK** na janela **ProtectTools**. Certifique-se de lembrar da senha gerada, pois não será possível desfazer uma configuração de senha sem fornecer a senha anterior.

Uma senha de ativação impede a utilização não autorizada do computador.

Nota Depois de definir uma senha de ativação, o botão **Configurar** em **Opções de senha** é substituído por um botão **Alterar**.

A senha de administrador do utilitário de configuração protege as configurações e as informações de identificação do sistema no utilitário de configuração. Depois de definida, essa senha deverá ser digitada para acessar o utilitário de configuração.

Caso não haja definida uma senha de administrador, a senha será solicitada antes que a parte de configuração do BIOS do ProtectTools se abra.

Nota Depois de definir uma senha de administrador, o botão **Configurar** em **Opções de senha** é substituído por um botão **Alterar**.

Definir a senha de ativação (se disponível)

Para definir a senha de ativação:

1. Selecione **Iniciar** > **Todos os programas** >**HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools)**.
2. No painel esquerdo, selecione **Configuração do BIOS** e depois selecione **Segurança**.
3. No painel direito, próximo à senha de **Ativação**, clique em **Configurar**.
4. Digite e confirme a senha nas caixas **Nova senha** e **Confirme senha**.
5. Clique em **OK** na caixa de diálogo **Senhas**.
6. Clique em **Aplicar**, depois clique em **OK** na janela **ProtectTools** para salvar suas alterações.

Alteração da senha de ativação (se disponível)

Para alterar a senha de ativação:

1. Selecione **Iniciar** > **Todos os programas** >**HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools)**.
2. No painel esquerdo, selecione **Configuração do BIOS** e depois selecione **Segurança**.

3. No painel direito, próximo à **Senha de ativação**, clique em **Alterar**.
4. Digite a senha atual na caixa **Senha atual**.
5. Digite e confirme a nova senha nas caixas **Nova senha** e **Confirme senha**.
6. Clique em **OK** na caixa de diálogo **Senhas**.
7. Clique em **Aplicar**, depois clique em **OK** na janela **ProtectTools** para salvar suas alterações.

Configuração de sistema

1. Inicializar o HP ProtectTools Embedded Security.
2. Inicializar chave de usuário básico.

O suporte à autenticação na ativação HP inicia assim que a chave básica de usuário e senha básica de usuário são definidas para a ativação. Depois da próxima reativação, o suporte à autenticação na ativação do HP ProtectTools é inicializado e a senha básica de usuário deve ser utilizada para iniciar o computador. Assim que o suporte à autenticação na ativação estiver funcionando, a opção para entrar na configuração do BIOS não é mais exibida. Se o usuário digita a senha de configuração na janela de suporte à autenticação na ativação, ele poderá entrar no BIOS.

Se a senha básica de usuário da embedded security já foi definida, então esta senha deve ser alterada para estabelecer a proteção por senha utilizando a autenticação na ativação.

Alteração do suporte à autenticação na ativação

O suporte à senha para autenticação na ativação utiliza a senha básica de usuário integrada. Para alterar a senha:

1. Entre nas configurações do BIOS F10 (deve ter a senha de configuração, conforme descrito nas etapas de configuração acima) e navegue até **Segurança** > **Dispositivo de embedded security** > **Restaurar credencial de autenticação**.
2. Pressione a tecla de cursor para alterara a configuração de **Não restaurar** para **Restaurar**.
3. Navegue até **Gerenciador de segurança)** > **Embedded Security** > **Configurações do usuário** > **Senha básica de usuário** > **Alterar**.
4. Digite a senha anterior, depois digite e confirme a nova senha.
5. Reiniciar no suporte à autenticação na ativação.

   A janela de senha solicita que o usuário digite a senha atual primeiro.
6. Digite a senha anterior, depois digite a nova senha. (Se for digitada a senha incorreta por três vezes, uma nova janela piscará informando que a senha é inválida e que a autenticação na ativação reverterá a senha original de embedded security F1 = Boot.

   Nesta altura, as senhas não serão sincronizadas e o usuário deve alterar a senha de embedded security novamente para sincronizá-las novamente.)

Alteração de contas de usuário

A autenticação na ativação oferece suporte apenas a um só usuário por vez. As seguintes etapas são utilizadas para alterar as contas de usuário que controlam a autenticação na ativação.

1. Navegue até **F10 BIOS** > **Segurança** > **Dispositivo de embedded security** > **Restaurar a credencial de autenticação**.
2. Pressione a tecla de seta para mover o cursor para os lados, depois pressione qualquer tecla para continuar.
3. Pressione F10 duas vezes, depois Enter para **Salvar configurações e sair**.
4. Crie/acesse uma mudança específica em usuário do Microsoft Windows.
5. Abra a embedded security e inicialize uma chave básica de usuário para a nova conta de usuário do Windows. Se já houver uma chave básica de usuário, alterar a senha básica de usuário para recuperar a propriedade da autenticação na ativação.

A autenticação na ativação agora aceita apenas a nova senha básica de usuário do novo usuário.

CUIDADO Muitos produtos estão disponíveis ao cliente para a proteção de dados por meio de criptografia de software, criptografia de hardware e hardware. A maioria deles é gerido por senhas. A falha em gerenciar estas ferramentas e senhas pode levar à perda de dados e bloqueio do hardware, o que pode exigir sua substituição. Reveja todos os arquivos de ajuda apropriados antes de tentar utilizar estas ferramentas.

Configuração da senha de administrador do utilitário de configuração

Para definir a senha de administrador do utilitário de configuração:

1. Selecione **Iniciar** > **Todos os programas** > **HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools)**.
2. No painel esquerdo, selecione **Configuração do BIOS** e depois selecione **Segurança**.
3. No painel direito, próximo à **Senha de configuração**, clique em **Configurar**.
4. Digite e confirme a senha nas caixas **Nova senha** e **Confirme senha**.
5. Clique em **OK** na caixa de diálogo **Senhas**.
6. Clique em **Aplicar**, depois clique em **OK** na janela **ProtectTools** para salvar suas alterações.

Alteração da senha de administrador do utilitário de configuração

Para alterar a senha de administrador do utilitário de configuração:

1. Selecione **Iniciar** > **Todos os programas** > **HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools)**.
2. No painel esquerdo, selecione **Configuração do BIOS** e depois selecione **Segurança**.
3. No painel direito, próximo à **Senha de configuração**, clique em **Alterar**.
4. Digite a senha atual na caixa **Senha atual**.
5. Digite e confirme a nova senha nas caixas **Nova senha** e **Confirme senha**.

6. Clique em **OK** na caixa de diálogo **Senhas**.
7. Clique em **Aplicar**, depois clique em **OK** na janela **ProtectTools** para salvar suas alterações.

Comportamento de ataque por dicionário com autenticação na ativação

Um ataque por dicionário é um método utilizado para invadir sistemas de segurança, testando sistematicamente todas as senhas possíveis para acessar o sistema de segurança. Um ataque por dicionário contra a embedded security tentaria detectar a senha do proprietário, a senha básica de usuário ou chaves protegidas por senha. A embedded security oferece uma defesa contra ataques por dicionário.

Defesa contra ataque por dicionário

A defesa contra ataques por dicionário da embedded security serve para detectar tentativas falhas de autenticação e desabilita temporariamente o TPM quando determinado limite de falhas for atingido. Uma vez atingido o limite de falhas, não só o TPM será desativado e uma reinicialização será feita, como os tempos-limites maiores de bloqueio são aplicados. Durante o tempo limite, se a senha correta for digitada, será ignorada. Se for digitada a senha incorreta, esta dobrará o último tempo-limite.

A documentação adicional sobre este processo está localizada na ajuda da embedded security. Clique em**Bem-vindo à solução HP Embedded Security para ProtectTools** > **Operação avançada de embedded security** > **Defesa contra ataques por dicionário**.

Nota Em geral, um usuário recebe aviso de que a senha está incorreta. Estes avisos informam quantas tentativas restaram ao usuário antes que o TPM seja desativado.

O processo de autenticação na ativação ocorre na memória ROM antes que o sistema operacional seja carregado. A defesa contra ataques por dicionário está operacional, porém o único aviso que o usuário receberá será o símbolo da tecla X.

2 HP para ProtectTools

Conceitos básicos

A configuração do BIOS para ProtectTools oferece o acesso às configurações de segurança e configuração do utilitário de configuração. Isso dá aos usuários Windows o acesso aos recursos de segurança do sistema que são gerenciados pelo utilitário de configuração.

Com a , é possível

- Gerenciar as senhas de ativação e as senhas de administrador.
- Configurar outros recursos de autenticação na ativação,tais como senhas de Java Card e suporte à autenticação da embedded security.
- Ativar e desativar os recursos de hardware, como o recurso de inicialização do CD-ROM ou portas diferentes de hardware.
- Configurar opções de inicialização que incluem ativar a inicialização múltiplas e alterar a seqüência de inicialização.

Nota A maioria dos recursos da configuração do BIOS para ProtectTools também estão disponíveis no utilitário de configuração.

Alteração das configurações do BIOS

A configuração do BIOS permite gerenciar várias configurações de computador que, em outro caso, seriam acessíveis somente se pressionar a tecla F10 durante a inicialização e acessar o utilitário de configuração. Consulte o *Guia do utilitário de configuração (F10) do computador* no *Documentation and Diagnostics CD (CD documentação e diagnósticos)* que vem com o computador para obter mais informações sobre como as configurações e recursos. Para acessar os arquivos de ajuda da configuração do BIOS, clique em **HP ProtectTools Security Manager (Gerenciador de segurança HP protectTools)** > **BIOS Configuration (Configuração do BIOS)** > **Ajuda**.

Nota Consulte as telas de ajuda do ProtectTools para instruções específicas sobre a BIOS Configuration do ProtectTools.

3 HP Embedded Security para ProtectTools

Conceitos básicos

Se disponível, o Embedded Security para ProtectTools protege contra o acesso não-autorizado aos dados ou credenciais do usuário. Este módulo oferece os seguintes recursos de segurança:

- Criptografia de arquivos e pastas pelo Enhanced Microsoft Encrypting File System (EFS).
- Criação de uma unidade segura pessoal (PSD) para criptografia de dados do usuário.
- Funções de gerenciamento de dados, tais como cópias de segurança e restauração da hierarquia principal.
- Suporte a aplicativos de terceiros que utilizam o MSCAPI (como o Microsoft Outlook e Internet Explorer) e aplicativos que utilizam o PKCS#11 (como o Netscape) para protegidas por certificados digitais ao utilizar o software de embedded security.

O chip embedded security TPM (Trusted Platform Module) otimiza e habilita outros recursos de segurança do HP ProtectTools Security Manager. Por exemplo, o Credential Manager para ProtectTools pode utilizar o chip embedded TPM como um fator de autenticação quando o usuário faz o logon no Windows. Em modelos selecionados, o chip embedded security TPM também ativa recursos avançados de segurança do BIOS, acessados através do BIOS Configuration para ProtectTools.

O hardware consiste em um TPM que atende aos requisitos do Trusted Computing Group dos padrões TPM 1.2 O chip é integrado com a placa de sistema. Algumas implementações do TPM (dependendo do modelo adquirido) integram o TPM como parte do NIC. Nestas configurações NIC e TPM, a memória no chip e fora do chip, funções e firmware estão localizados em um cartão flash externo integrado com a placa de sistema. Todas as funções TPM são criptografadas ou protegidas para garantir o flash ou comunicações seguras.

O software também oferece uma função denominada PSD. PSD é uma função adicional à criptografia de arquivo/pasta com base em EFS, e utiliza o algoritmo de criptografia Advanced Encryption Standard (AES). É importante notar que o HP ProtectTools Personal Secure Drive não pode funcionar a menos que o TPM esteja visível (não oculto), ativado com o software adequado instalado com propriedade a configuração de usuário for inicializada.

Procedimentos de configuração

CUIDADO Para reduzir o risco de segurança, é altamente recomendável que o administrador de TI inicialize imediatamente o chip embedded security TPM. Se o chip embedded security TPM não for inicializado, um usuário não-autorizado ou worm de computador pode obter acesso ao mesmo, ou um vírus pode inicializar o chip embedded security TPM e restringir o acesso ao PC.

O chip embedded security TPM pode ser ativado no utilitário BIOS Configuration do computador, BIOS Configuration para ProtectTools ou o HP Client Manager.

Para ativar chip embedded security TPM:

1. Abra o utilitário de configuração ligando ou reiniciando o computador e em seguida, pressione F10 enquanto a mensagem **F10 = ROM Based Setup** (F10 = Configuração com base na memória ROM) é exibida no canto inferior esquerdo da tela.
2. Utilize as teclas de seta para selecionar **Segurança** > **Senha de configuração**. Defina uma senha.
3. Selecione **Dispositivo embedded security**.
4. Utilize as teclas de seta para selecionar **Dispositivo de embedded security – Desativar**. Utilize as teclas de seta para alterar para **Dispositivo embedded security – Ativar**.
5. Selecione **Ativar** > **Salvar alterações e sair**.

Nota Consulte as telas de ajuda do ProtectTools para instruções específicas sobre o ProtectTools Embedded Security.

4 HP Credential Manager para ProtectTools

Conceitos básicos

O Credential Manager para ProtectTools possui recursos de segurança que oferecem um ambiente computacional seguro e conveniente: Estes recursos incluem:

- Alternativas de senhas quando efetuar o logon no Microsoft Windows, como a utilização de um Java Card ou leitor biométrico.
- Recurso de acesso único que lembra automaticamente as credenciais (IDs de usuário e senhas) para web sites, aplicativos e recursos de rede protegidos.
- Suporte para dispositivos de segurança opcionais, como Java Cards e leitores biométricos.
- Suporte para configurações adicionais de segurança. como exigir uma autenticação com um dispositivo opcional de segurança para desbloquear o computador e acessar os aplicativos.
- Criptografia otimizada para senhas armazenadas, quando implementado com o chip embedded security TPM.

Procedimento de lançamento

Para iniciar o Credential Manager, se disponível:

1. Clique em **Iniciar** > **Painel de controle** > **Centro de segurança** > **HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools)** > **Credential Manager**.
2. Clique em **Fazer logon** na parte superior direita do painel.

Também é possível acessar o Credential Manager das seguintes maneiras:

- Credential Manager Logon Wizard (Assistente de login do Credential Manager)(preferível)
- ProtectTools Security Manager

Nota Caso a solicitação de login do Credential Manager seja utilizado na tela de login do Windows para fazer o login no Credential Manager, o usuário também estará acessando o Windows.

Acesso pela primeira vez

Na primeira vez em que o Credential Manager é aberto, o usuário faz o logon com a senha de login normal do Windows. Uma conta Credential Manager é automaticamente criada com as credenciais de login do Windows.

Após o login no Credential Manager, o usuário pode registrar credenciais adicionais, como uma impressão digital ou Java Card.

No próximo login, é possível selecionar o criterio de login e utilizar qualquer combinação das credenciais registradas.

Nota Consulte as telas de ajuda do ProtectTools para instruções específicas sobre o ProtectTools Security Manager.

5 HP Java Card Security para ProtectTools

Conceitos básicos

O Java Card Security para ProtectTools gerencia a instalação e configuração do Java Card para computadores equipados com um leitor opcional de Java Card.

Com a Java Card Security para ProtectTools, é possível:

- Acessar os recursos de segurança do Java Card.
- Inicializar um Java Card de forma que ele possa ser utilizado com outros módulos do ProtectTools, tais como o Credential Manager para ProtectTools.
- Se disponível, trabalhar com utilitário de configuração para habilitar a autenticação por Java Card em um ambiente antes da inicialização e configurar os Java Cards individuais para um administrador e para um usuário. Isso exige que um usuário insira o Java Card e, de forma opcional, informe um PIN antes de permitir que o sistema operacional seja carregado.
- Se disponível, definir e alterar a senha utilizada para autenticar os usuários do Java Card.
- Se disponível, realizar o backup e restaurar senhas de BIOS Java Card armazenadas no Java Card
- Se disponível, salvar a senha do BIOS no Java Card

Nota Consulte as telas de ajuda do ProtectTools para instruções específicas sobre o HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools).

6 Soluções de terceiros

As plataformas que contém um TMP exigem ambos TGC Softawre Stack (TTS) e o software de embedded security. Todos os modelos oferecem o TSS; o software embedded security deve ser adquirido separadamente para alguns modelos. Para estes modelos, é fornecido um NTRU TSS para oferece suporte à aquisição de software embedded security de terceiros. Recomendamos soluções de terceiros tais como o Wave Embassy Trust Suíte.

7 HP Client Manager para Remote Deployment (Gerenciador de HP cliente para implementação remota)

Histórico

As plataformas HP Trustworthy equipadas com um modulo Trusted Platform (TPM), são fornecidas com o TPM desativado (estado padrão). Ativar o estado do TPM é uma opção administrativa protegida por meio de criterios reforçadas do BIOS HP. O administrador precisa estar na frente da máquina para inserir as opções da (Opções F10) para ativar o TPM. Além disso, as especificações do Trusted Computing Group (TCG) exigem que, para ligar o TPM, é necessário estabelecer uma presença humana explícita (física). Isso existe principalmente para assegurar que os direitos de privacidade do usuário sejam respeitados (ao fornecer um modelo OPCIONAL para utilização), bem como assegurar que aplicativos não-autorizados, vírus ou cavalos de tróia não ativem o TPM para utilização maliciosa. O estabelecimento da presença física e a necessidade da presença local de um administrador apresentam desafios interessantes para os gerentes de TI que estão tentando implementar essa tecnologia através de uma grande empresa.

Inicialização

O HP Client Manager (HPCM) oferece um método de ativação remota do TPM e traz a propriedade do TPM para o ambiente da empresa. Este método não requer a presença física do administrador e TI, embora ainda cumpra com a exigência do TCG.

O HPCM permite ao administrador de TI definir certas opções de BIOS e depois reiniciar o sistema para ativar o TPM no sistema remoto. Durante a reinicialização, a BIOS, por padrão, exibe uma solicitação; em resposta, o usuário final precisa pressionar uma tecla para provar sua presença física, como especificado pelo TCG. O sistema remoto prossegue com a inicialização e o script conclui assumindo a propriedade do TPM no sistema. Durante esse procedimento são criados um arquivo e uma token de recuperação de emergência em um local determinado pelo administrador de TI.

O HPCM não executa a inicialização do usuário TPM no sistema remoto, uma vez que o usuário precisa escolher a senha. A inicialização de usuário TPM deve ser realizada pelo usuário final desse sistema.

Manutenção

O HP Client Manager (Gerenciador de HP cliente) pode ser utilizado para restaurar a senha de usuário remotamente, sem que o administrador de TI tenha conhecimento da senha de usuário. O HP Client Manager (Gerenciador de HP cliente) também pode recuperar remotamente as credenciais de usuário. As senhas de administrador adequadas devem ser fornecidas para ambas as funções.

8 Solução de problemas

para ProtectTools

Descrição resumida	Detalhes	Solução
Ao utilizar a opção contas de rede do Credential Manager, um usuário pode selecionar em qual conta de domínio deseja efetuar o logon. Quando a autenticação TPM é utilizada, esta opção não está disponível. Todos os outros métodos de autenticação funcionam normalmente.	Ao utilizar a autenticação TPM, o usuário efetua o logon apenas no computador local.	A utilização das ferramentas de único logon do Credential Manager permite ao usuário autenticar outras contas.
A credencial por token USB não está disponível com o login no Windows XP Service Pack 1.	Após instalar o software de token USB, registrar a credencial por token USB e configurar o Credential Manager como login primário, o Token USB não será listado, tampouco estará disponível no Credential Manager/gina logon Ao efetuar o logon de novo no Windows, efetuar o logoff do Credential Manager, e voltar a efetuar o logon no Credential Manager e selecionar novamente o token como login primário, a opção de login por token opera normalmente.	Isso ocorre apenas com o Windows XP Service Pack 1; atualize a versão de Windows para o Service Pack 2 via Windows Update para corrigir. Para contornar o problema e permanecer com o Service Pack 1, faça novo login no Window sutilizando outra credencial (senha do Windows) para poder efetuar o logoff e novo logon no Credential Manager.
Algumas páginas de aplicativos com base na web geram erros que impedem o usuário de realizar ou concluir tarefas.	Alguns aplicativos com base na web param de funcionar e geram erros devido à desativação do padrão de funcionalidade de acesso único. Por exemplo, um **!** em um triângulo amarelo é observado no Internet Explorer como uma indicação de ocorrência de erro.	O acesso único do Credential Manager não oferece suporte para todas as interfaces web. Desative o suporte para o acesso único para páginas específicas da Web, desativando o suporte ao acesso único. Consulte a documentação completa sobre o acesso único, que está disponível nos arquivos de ajuda do Credential Managrer. Se um acesso único específico não puder ser desativado para certo aplicativo, contate o Serviço e Suporte HP e solicite suporte de terceiro nível por meio de seu contato de serviço HP.
Nenhuma opção para **Procurar por token virtual** durante o processo de logon.	O usuário não pode mover o local do token virtual registrado no Credential Manager pois a opção para procurar foi removido por causa de riscos à segurança.	A opção procurar foi removida das ofertas atuais do produto por permitia que usuários não-autorizados excluíssem e renomeassem arquivos e obtivessem o controle do Windows.

Descrição resumida	Detalhes	Solução
O acesso com a autenticação TPM não oferece a opção **Contas de rede**.	Ao utilizar a opção **Contas de rede**, um usuário pode selecionar em qual conta de domínio deseja efetuar o logon. Quando a autenticação TPM é utilizada, esta opção não está disponível.	A HP está pesquisando uma solução alternativa para aprimoramentos futuros do produto.
Os administradores de domínio não podem alterar a senha do Windows, mesmo com autorização.	Isso ocorre depois que um administrador de domínio acessar um domínio e registra a identidade do domínio com o Credential Manager, utilizando uma conta com privilégios de administrador no domínio e no computador local. Quando o administrador de domínio tenta alterar a senha do Windows a partir do Credential Manager, ele obtém uma falha de erro de login: **Restrição de conta de usuário**.	O HP Credential Manager não pode alterar uma senha de conta de usuário de domínio por meio da função **Alterar senha do Windows**. O HP Credential Manager pode alterar apenas as senhas de conta do computador local. O usuário do domínio pode alterar sua senha por meio da opção **Segurança do Windows** > **Alterar senha**, mas, uma vez que o usuário de domínio não possui uma conta física no computador local, o Credential Manager só pode altera a senha utilizada para efetuar o logon.
As configurações padrão de acesso único do Credential Manager podem ser solicitadas para evitar loop.	O acesso único padrão é definido para registrar automaticamente o acesso dos usuários. Entretanto, ao criar o segundo de dois documentos distintos protegidos por senha, o Credential Manager utiliza a última senha gravada-aquela do primeiro documento.	A HP está pesquisando uma solução alternativa para aprimoramentos futuros do produto.
Problemas de incompatibilidade com a senha gina do Corel WordPerfect 12.	Se o usuário tenta acessar o Credential Manager, criar m documento no WordPerfect e salvar com proteção por senha, o Credential Manager não consegue detectar o reconhecer, seja manual ou automaticamente, a senha gina.	A HP está pesquisando uma solução alternativa para aprimoramentos futuros do produto.
O Credential Manager não reconhece o botão **Conectar** na tela.	Se as credenciais de acesso único do Remote Desktop Connection (RDP) forem definidas em **Conectar**, Acesso único, na reinicialização, selecione sempre **Salvar como** em vez de **Conectar**.	A HP está pesquisando uma solução alternativa para aprimoramentos futuros do produto.
Assistente de configuração do ATI Catalyst não pode ser utilizado com o Credential Manager.	O acesso único do Credential Manager causa conflitos com o assistente de configuração do ATI Catalyst.	Desativar o acesso único do Credential Manager.
Ao efetuar o logon utilizando a autenticação TPM, o botão **Voltar** na tela pula a opção de escolher outro método de autenticação.	Se um usuário utilizando a autenticação de login TPM para o Credential Manager introduzir sua senha, o botão **Voltar** não funciona corretamente, em vez disso, exibe imediatamente a tela de logon do Windows.	A HP está pesquisando uma solução alternativa para aprimoramentos futuros do produto.
O Credential Manager abre durante o modo em espera, mesmo quando configurado para não fazê-lo.	Quando **utilizar login do Credential Manager no Windows** não estiver selecionado como uma opção, permitindo que o sistema entre modo de suspensão S3 e depois seja reativado faz com que o login do Credential Manager para o Windows se abra.	Sem uma senha de administrador definida, o usuário não pode acessar o Windows através do Credential Manager por causa das restrições de conta invocadas pelo mesmo. • Sem Java Card/token, o usuário pode cancelar o logon do Credential Manager e o usuário irá ver o

Descrição resumida	Detalhes	Solução
		login do Windows. Nesta altura, o usuário consegue efetuar o logon. • Com Java Card/token, as seguintes soluções alternativas permitem que o usuário ative/desative a abertura do Credential Manager mediante a inserção do Java Card. 1. Clique na guia **Configurações avançadas**. 2. Clique em **Serviço e aplicativos**. 3. Clique em **Java Cards e Tokens**. 4. Clique quando o Java Card/token for inserido. 5. Marque a caixa de seleção **Alerta para logon**.
Se o modulo TPM for removido ou danificado, os usuários perderão todas as credenciais do Credential Manager protegidas pelo TPM.	Se o modulo TPM for removido ou danificado,os usuários perderão todas as credenciais protegidas pelo TPM.	Isso foi projetado desta maneira. O modulo TPM foi projetado para proteger as credenciais do Credential Manager. A HP recomenda que o usuário faça o backup de identidade do Credential Manager antes de remover o módulo TPM.
Credential Manager não configurado como logon primário no Windows 2000.	Durante a instalação do Windows 2000, a política de logon é definida como admin de logon manual ou automático. Se for escolhido o login automático, as configurações padrão de registro do Windows define o valor do login automático de administrador em 1, e o Credential Manager não ignora isso.	Isso foi projetado desta maneira. Se o usuário deseja modificar as configurações de nível de sistema operacional para os valores de login automático de administrador para ignorar, o caminho de edição é `HKEY_LOCAL_MACHINE/Software/Microsoft/ WindowsNT/CurrentVersion/WinLogon` **CUIDADO** Utilize o editor de registro por sua própria conta e risco! O uso indevido do editor de registro (regedit) pode causar sérios problemas que exigirão a reinstalação do sistema operacional. Não há garantias de que os problemas resultantes da má utilização do editor de registro possam ser resolvidos.
A mensagem de login por impressão digital aparece independente da instalação ou registro de um leitor de impressões digitais.	Se o usuário selecionar o logon do Windows, o seguinte alerta de área de trabalho aparece na barra de tarefas do Credential Manager. **Também é possível acessar o Credential Manager através do leitor de impressão digital.**	A finalidade do alerta da área de trabalho é notificar o usuário de que a autenticação por impressão digital está disponível, se estiver configurada.
A janela de logon do Credential Manager para o Windows 2000 diz **insira** o cartão enquanto não há nenhum leitor instalado.	A tela de boas-vindas do Credential Manager do Windows sugere que o usuário pode efetuar o logon com **insira o cartão** enquanto não há nenhum leitor de Java Card instalado.	A finalidade do alerta é notificar o usuário de que a autenticação por Java Card está disponível, se estiver configurada.
Não é possível efetuar o login no Credential Manager depois de passar de modo de suspensão para modo de hibernação apenas no	Depois de passar o sistema de modo de hibernação e suspensão, o Administrador ou o usuário não consegue efetuar o login no Credential Manager, e a tela de login do Windows permanece exibida, independente da	Este problema parece ter sido resolvido no Service Pack 2 da Microsoft. Consulte a base de conhecimentos da Microsoft, artigo 813301 em http://www.microsoft.com para mais informação sobre a causa deste problema.

Descrição resumida	Detalhes	Solução
Windows XP Service Pack 1.	credencial de login (senha, impressão digital ou Java Card) selecionada.	Para efetuar o logon, o usuário deve selecionar o Credential Manager e efetuar o login. Depois de acessar o Credential Manager, o usuário deve efetuar o login no Windows (ele terá que selecionar a opção de logon do Windows) para concluir o processo de login. Se o usuário acessar antes o Windows, então terá que acessar manualmente o Credential Manager.
A restauração do Embedded Security causa uma falha no Credential Manager.	O CM não registra credenciais depois que a ROM é restaurada com as configurações de fábrica.	O HP Credential Manager for ProtectTools não consegue acessar o TPM se a ROM tiver sido restaurada com as configurações de fábrica após a instalação do Credential Manager. O chip embedded security TPM pode ser ativado no Utilitário do BIOS de Configuração do Computador, BIOS Configuration para ProtectTools ou o HP Client Manager. Para ativar chip embedded security TPM: 1. Abra o utilitário de Configuração ligando ou reiniciando o computador e em seguida, pressione F10 enquanto a mensagem **F10 = ROM Based Setup** (F10 = Configuração com Base na Memória ROM) é exibida no canto inferior esquerdo da tela. 2. Utilize as teclas de seta para selecionar **Segurança** > **Senha de Configuração**. Defina uma senha. 3. Selecione **Dispositivo de embedded security**. 4. Utilize as teclas de seta para selecionar **Dispositivo de embedded security – Desativar**. Utilize as teclas de seta para alterar para **Dispositivo de embedded security – Ativar**. 5. Selecione **Ativar** > **Salvar alterações e sair**. A HP está investigando as opções de solução para futuros lançamentos de software ao cliente.
O processo de segurança **Restaurar identidade** perde a associação com o token virtual.	Quando o usuário restaura a identidade, o Credential Manager perde a associação com o local do token virtual na tela de logon. Mesmo que o Credential Manager tenha um token virtual registrado, o usuário de registrar novamente o token par restaurar a associação.	Esta é uma decisão de projeto. Ao desinstalar o Credential Manager sem manter as identidades, o a parte de sistema (servidor) do token é destruída, de forma que ele não pode mais ser utilizado para efetuar o logon, mesmo que a parte cliente do token seja restaurada por meio de restauração de identidade. A HP está investigando as opções longo prazo para a solução.

Embedded Security for ProtectTools

Descrição resumida	Detalhes	Solução
Criptografia de pastas, sub-pastas e arquivos no PSD gera mensagem de erro.	Se o usuário copiar arquivos e pastas para o PSD e tentar codificá-los, a mensagem de erro **Erro ao aplicar atributos** é exibida. O usuário pode codificar os mesmos arquivos na unidade C:\ em uma unidade de disco rígido adicional instalada.	Isso foi projetado desta maneira. Mover pastas/arquivos para o PSD automaticamente causa sua codificação. Não é necessário codificar duas vezes os arquivos e pastas. Ao tentar efetuar uma dupla codificação utilizando o PSD, o EFS produzirá esta mensagem de erro.
Não é possível assumir a propriedade com outro sistema operacional na plataforma MultiBoot.	Se uma unidade estiver configurada para inicialização de múltiplos sistemas operacionais, a propriedade só pode ser definida com o assistente de inicialização de plataforma em um sistema operacional.	Esta é uma decisão de projeto por questões de segurança.
Um administrador não autorizado pode visualizar, excluir, renomear ou mover o conteúdo de pastas EFS criptografadas.	A criptografia de uma pasta não impede um usuário não autorizado com privilégios administrativos de visualizar, excluir, renomear ou mover o conteúdo da pasta.	Isso foi projetado desta maneira. Este é um recurso do EFS não do Embedded Security TPM. O Embedded Security utiliza o software EFS da Microsoft e preserva os direitos de acesso a pastas/ arquivos para todos os administradores.
As pastas criptografadas com EFS no Windows 2000 não são exibidas em realce verde.	As pastas criptografadas com EFS são exibidas com um realce verde no Windows XP, mas não no Windows 2000.	Isso foi projetado desta maneira. Este é um recurso do EFS que não realça as pastas criptografadas no Windows 2000, mas o faz no Windows XP. Isso ocorre mesmo que não haja um Embedded Security TPM instalado.
O EFS não exige uma senha para exibir arquivos criptografados no Windows 2000.	Se o usuário configura o Embedded Security, acessar como administrador e depois troca de usuário e volta como administrador, o usuário poderá, subsequentemente, visualizar arquivos e pastas no Windows 2000 sem uma senha. Isso ocorre somente na primeira conta de administrador no Windows 2000. Ao utilizar uma segunda conta de administrador, este problema não ocorre.	Isso foi projetado desta maneira. Este é um recurso do EFS no Windows 2000. O EFS no Windows XP, por padrão, não permite que o usuário abra arquivos/pastas sem uma senha
O software não deve ser instalado em uma restauração com partição FAT32.	Se o usuário tentar restaurar a unidade de disco rígido utilizando o FAT32, não haverá opções de criptografia para qualquer arquivo/pasta utilizando o EFS.	Esta foi uma decisão de projeto. O EFS da Microsoft é admitido apenas em NTFS e não funcionará em FAT32. Este é um recurso do EFS da Microsoft e não está relacionado ao software HP ProtectTools.
O usuário do Windows 2000 pode compartilhar com a rede qualquer PSD com um compartilhamento ($) oculto.	O usuário do Windows 2000 pode compartilhar com a rede qualquer PSD com um compartilhamento ($) oculto. O compartilhamento oculto pode ser acessado via rede utilizando o compartilhamento ($) oculto.	O PSD normalmente não é compartilhado em rede, porém pode ser feito via compartilhamento ($) oculto somente no Windows 2000. A HP recomenda ter sempre a conta de administrador protegida por senha.
O usuário é capaz de codificar ou excluir o arquivo XML do arquivo de recuperação.	Por padrão, os ACLs desta pasta não estão definidos; assim, um usuário pode inadvertidamente ou intencionalmente criptografar ou excluir o arquivo, tornando-o inacessível. Uma vez	Esta foi uma decisão de projeto. Os usuarios tem privilégios de acesso a um arquivo de emergência para salvar/atualizar sua copia de segurança da chave básica de usuário. Os clientes são encorajados a adotar uma abordagem de segurança

Descrição resumida	Detalhes	Solução
	criptografado ou excluído este arquivo, ninguém poderá utilizar o software TPM.	de melhores práticas e instruir seus usuários a nunca criptografar ou excluir arquivos de recuperação.
A interação do HP ProtectTools Embedded Security EFS com o Symantec Antivirus ou Norton Antivirus prolongam os tempos de codificação/decodificação e varredura.	Os arquivos criptografados interferem com a varredura de vírus do Symantec Antivirus ou Norton Antivirus 2005. Durante o processo de varredura, a solicitação de senha básica de usuário pede a senha ao usuário a cada 10 ou mais arquivos. Se o usuário não digitar uma senha, a solicitação de senha básica de usuário expira, permitindo que o NAV2005 continue com a varredura. A criptografia de arquivos com o HP ProtectTools Embedded Security EFS demora mais quando o Symantec Antivirus ou Norton Antivirus estão em execução.	Para reduzir o tempo necessário para varrer os arquivos HP ProtectTools Embedded Security EFS, o usuário pode digitar a senha de criptografia antes de iniciar a varredura e decodificar os arquivos antes da varredura. Para reduzir o tempo necessário para codificar/decodificar os dados utilizando o HP ProtectTools Embedded Security EFS, o usuário deve desativar a Proteção Automática no Symantec Antivirus ou Norton Antivirus.
Não consegue salvar o arquivo de recuperação de emergência em mídia removível	Se o usuário inserir um cartão MMC ou SD ao criar um caminho para o arquivo de recuperação de emergência durante a inicialização do Embedded Security, uma mensagem de erro é exibida.	Esta foi uma decisão de projeto. O armazenamento do arquivo de arquivo de recuperação em mídia removível não é admitido. O arquivo de recuperação pode ser armazenado em uma unidade de rede ou outra unidade local que não seja a unidade C.
Não é possível codificar dados no ambiente do Windows 2000 Francês (França).	Não há uma seleção **Codificar** ao clicar com o botão direito do mouse sobre um ícone de arquivo.	Esta é uma limitação do sistema operacional da Microsoft. Se a região for alterada para outra qualquer (Francês (Canadá), por exemplo), aí a seleção **Codificar** aparecerá. Para contornar o problema, codifique o arquivo da seguinte forma: Clique com o botão direito no ícone do arquivo e selecione **Propriedades** > **Avançado** > **Codificar Conteúdo**.
Ocorrem erros após uma queda de energia, durante a tomada de propriedade na inicialização do Embedded Security.	Se houver uma queda de queda de energia durante a inicialização do chip Embedded Security, os seguintes problemas ocorrerão: • Ao tentar iniciar o Assistente de Inicialização do Embedded Security, o seguinte erro é exibido: **O Embedded Security não pode ser inicializado uma vez que o chip Embedded Security já tem um proprietário Embedded Security.** • Ao tentar iniciar o assistente de inicialização de usuário, o seguinte erro é exibido: **O Embedded Security não foi inicializado. Para utilizar o assistente, o Embedded Security precisa ser inicializado antes.**	Execute o procedimento a seguir para recuperar depois de uma queda de energia: **Nota** Utilize as teclas de seta para selecionar vários menus, itens de menu e para alterar valores (salvo outra especificação). 1. Ligue ou reinicie o computador. 2. Pressione F10 quando a mensagem **F10=Setup** for exibida na tela (ou assim que o LED do monitor ficar verde). 3. Selecione a opção de idioma apropriada. 4. Pressione Enter. 5. Selecione **Segurança** > **Embedded Security**. 6. Defina a opção **Dispositivo Embedded Security** como **Ativar**. 7. Pressione F10 para aceitar a alteração. 8. Selecione **Arquivo** > **Salvar alterações e sair**.

Descrição resumida	Detalhes	Solução
		9. Pressione ENTER. 10. Pressione a tecla F10 para salvar as alterações e sair do utilitário de configuração F10.
A senha do utilitário de configuração (F10) pode ser removida depois de ativar o módulo TPM.	A ativação do módulo TPM requer uma senha do utilitário de configuração (F10). Com o módulo ativado, o usuário pode remover a senha. Isso permite que qualquer pessoa com acesso direto ao sistema restaure o módulo TPM e causar uma possível perda de dados.	Esta foi uma decisão de projeto. A senha do utilitário de configuração (F10) só pode ser removida por um usuário que conheça a senha. Todavia, a HP recomenda proteger constantemente a senha do utilitário de configuração (F10).
A caixa para a senha PSD não é exibida quando o sistema é restaurado do status em espera.	Quando um usuário efetua o logon no sistema após criar um PSD, o TPM solicita a senha básica de usuário. Se o usuário não inserir a senha e o sistema entrar em espera, a caixa de diálogo de senha não está mais disponível assim que o usuário retorna.	Esta é uma decisão de projeto. O usuário precisa efetuar o logoff e novo logon para visualizar novamente a caixa de senha PSD.
Nenhuma senha é necessária para alterar os criterios de segurança da plataforma.	O acesso às políticas de segurança da plataforma (tanto máquina como usuário) não exige uma senha TPM para usuários com privilégios administrativos no sistema.	Esta é uma decisão de projeto. Qualquer administrador pode modificar as políticas de segurança da plataforma com ou sem a inicialização de usuário TPM.
O Microsoft EFS não funciona corretamente no Windows 2000.	Um administrador pode acessar informações codificadas no sistema sem saber a senha correta. Se o administrador inserir uma senha incorreta ou cancelar o diálogo de senha, o arquivo codificado poderá ser aberto como se o administrador tivesse digitado a senha correta. Isso ocorre independente das configurações de segurança utilizadas na criptografia dos dados. Isso ocorre somente com a primeira conta de administrador no Windows 2000.	O criterio de recuperação de dados é automaticamente configurada para determinar um administrador como um agente de recuperação. Quando uma chave de usuário não pode ser recuperada (como no caso de digitação de senha incorreta ou cancelamento do diálogo para digitar senha), o arquivo é automaticamente decodificado com a chave de recuperação. Isso é causado pelo Microsoft EFS. Consulte a base de conhecimentos da Microsoft, artigo técnico Q257705 em http://www.microsoft.com para mais informação. Os documentos não podem ser abertos por usuário sem privilégios administrativos.
Ao visualizar um certificado, ele exibe como não-confiável.	Depois de configurar o HP ProtectTools e executar o assistente de inicialização de usuário, o usuário pode visualizar o certificado emitido; entretanto, ao visualizar o certificado, ele é exibido como não-confiável. Embora o certificado possa ser instalado a esta altura, clicando no botão Instalar, a instalação não o torna confiável.	Os certificados auto-assinados não são confiáveis. Em um ambiente empresarial devidamente configurado, os certificados EFS são emitidos pelas autoridades de certificação online e são considerados confiáveis.
Ocorre o erro de codificação e decodificação intermitente: **O processo não pode acessar o arquivo, pois ele está sendo utilizado por outro processo.**	Erro extremamente intermitente durante a codificação ou decodificação de arquivos, gerada quando o arquivo está em uso por outro processo, mesmo que o arquivo ou pasta em questão não estejam sendo processado pelo sistema operacional ou outros aplicativos.	Para resolver a falha: 1. Reinicie o sistema. 2. Efetue o log off. 3. Efetue novo logon
A perda de dados em armazenamento	A remoção de mídias de armazenamento como uma unidade de	O problema ocorre somente se o usuário acessar o PSD, depois remove a unidade de disco rígido antes

Descrição resumida	Detalhes	Solução
removível ocorre se o armazenamento for removido antes da geração ou transferência dos novos dados.	disco rígido MultiBay ainda mostra a disponibilidade PSD e não gera erros ao adicionar/modificar dados no PSD. Após reiniciar o sistema, o PSD não reflete as alterações de arquivo que ocorreram enquanto a mídia removível não estava disponível.	de concluir a geração ou transferência de novos dados. Se o usuário tenta acessar o PSD sem a presença da unidade de disco rígido removível, uma mensagem de erro é exibida, informando que o **dispositivo não está pronto**.
Durante a desinstalação, se o usuário não inicializar o usuário básico e abrir a ferramenta de administração, a opção **Desativar** não estará disponível e o desinstalador não continuará até que a ferramenta de administração seja fechada.	O usuário tem a opção de desinstalar, seja sem desativar o TPM, ou desativando antes o TPM (por meio da ferramenta de administração) e depois, desinstalando. O acesso à ferramenta administração requer a inicialização da chave básica de usuário. Se não ocorrer a inicialização básica, todas as opções estarão inacessíveis ao usuário. Visto que o usuário explicitamente optou por abrir a ferramenta administração (clicando na caixa de diálogo **Sim** da solicitação **Clique em Sim para abrir a ferramenta de administração do Embedded Security**), a desinstalação aguarda até o encerramento da ferramenta administração. Se o usuário clicar em **Não** nessa caixa de diálogo, a ferramenta administração não abrirá e a desintalação continua.	A ferramenta administração é utilizada para desativar o chip TPM, mas essa opção não está disponível a menos que a chave básica de usuário tenha sido inicializada. Se não foi inicializada, selecione **OK** ou **Cancelar** para continuar com o processo de desinstalação.
Bloqueio de sistema intermitente ocorre apos criar PSD em duas contas de usuário e utilizando a troca rápida de usuários em configurações de sistema de 128 MB.	O sistema pode travar em uma tela preta e sem resposta no teclado ou mouse em vez de exibir a tela de boas-vindas (logon), quando a troca rapida de usuários é utilizada com mínima RAM.	A suspeita de causa raiz é um problema de sincronização nas configurações da memória baixa. Os gráficos integrados utilizam a arquitetura UMA, que consome 8 MB de memória, deixando apenas 120 disponíveis ao usuário. Estes 120 MB são compartilhados por ambos usuários que estão acessando o sistema e estão efetuando a troca rápida de usuários quando o erro é gerado. A solução alternativa é reiniciar o sistema e o cliente é recomendado a aumentar a configuração de memória (a HP não oferece configurações de 128 MB por padrão com módulos de segurança).
A Autenticação de Usuário EFS (solicitação de senha) expira com **acesso negado**.	A senha de autenticação de usuário EFS reabre após clicar em **OK** ou apos retornar do estado de espera após expirar.	Esta é uma decisão e projeto para evitar problemas com o MS EFS, onde um watchdog timer de 30 segundos foi criado para gerar a mensagem de erro).
Pequenos truncamentos durante a instalação em japonês foram observados na descrição funcional.	As descrições funcionais durante aa opções de configuração personalizada, durante o assistente de instalação, estão truncadas.	A HP corrigirá este problema em uma versão futura.
A criptografia EFS funciona sem digitar a senha.	A criptografia ainda pode ser realizada em um arquivo ou pasta mesmo após expirar a solicitação de senha do usuário.	A capacidade em criptografiar não exige autenticação de senha, uma vez que este é um recurso da criptografia Microsoft EFS. A decodificação exigirá a senha do usuário.
O email protegido é admitido, mesmo se desmarcado no assistente	O software de embedded security e o assistente não controlam as	Este é um comportamento projetado. A configuração de definições de email do TPM não proíbe a edição das configurações de criptografia diretamente no cliente de

Descrição resumida	Detalhes	Solução
de inicialização de usuário ou se a configuração de email seguro estiver desativada nas políticas de usuário.	configurações de um cliente de email (Outlook, Outlook Express ou Netscape)	email. O uso de email seguro é definido e controlado por aplicativos de terceiros. O assistente HP permite vínculos a três aplicativos de referência para personalização imediata.
A execução de implantação em larga escala por uma segunda vez no mesmo PC ou em um PC previamente inicializado sobregrava os arquivos de recuperação de emergência e de token de emergência. Os novos arquivo não servem para recuperação.	A execução de implantação em larga escala em um sistema HP ProtectToosl Embedded Security previamente inicializado danificará os arquivos de recuperação e de token de recuperação, sobregravando estes arquivos xml.	A HP está trabalhando para resolver o problema de sobregravação de arquivo xlm e oferecerá uma solução em um SoftPaq futuro.
Scripts de logon automáticos não funcionam durante a restauração de usuário no Embedded Security.	O erro ocorre depois que o usuário • Inicializa o proprietário e usuário no Embedded Security (utilizando os locais padrão – **Meus documentos**). • Restaure o chip com as configurações de fábrica no BIOS. • Reinicia o computador. • Começa a restaurar o Embedded Security. Durante o processo de restauração, o Credential Manager pergunta ao usuário se o sistema pode automatizar o logon na autenticação de usuário TPM Infineon. Se o usuário seleciona **Sim**, então o local de SPEmRecToken aparece automaticamente na caixa de texto. Mesmo que este local esteja correto, a seguinte mensagem de erro é exibida: **Nenhum token de recuperação de emergência foi fornecido. Selecione o local do para recuperação do token de recuperação de emergência.**	Clique no botão **Procurar** na tela para selecionar o local e o processo de restauração continuará.
PSDs de múltiplos usuário não funcionam em um ambiente com troca rápida de usuário.	Este erro ocorre quando múltiplos usuários são criados e recebem um PSD com a mesma letra de unidade. Ao tentar efetuar a troca rápida de usuário com o PSD carregado, o PSD do segundo usuário não estará disponível.	O PSD do segundo usuário só estará disponível se for reconfigurado para utilizar outra letra de unidade, ou se o primeiro usuário efetuar o logoff.
O PSD é desativado é não pode ser excluído depois de formatar a unidade de disco rígido onde o PSD foi gerado.	O PSD é desativado é não pode ser excluído depois de formatar a unidade de disco rígido secundária onde o PSD foi gerado. O ícone do PSD ainda está visível, mas a mensagem de erro **a unidade não está acessível** aparece quando o usuário tenta acessar o PSD.	Conforme decisão de projeto: Se um cliente força a exclusão ou desconecta do local de armazenamento dos dados PSD, a emulação de unidade PSD do Embedded Security continuará a funcionar e produzirá erros com base na ausência de comunicação com os dados faltantes.

Descrição resumida	Detalhes	Solução
	O usuário não consegue excluir o PSD e uma mensagem aparece dizendo: **seu PSD ainda está em uso, certifique-se de que o PSD não contém arquivos abertos e que não está sendo acessado por nenhum outro processo**. O usuário deve reiniciar o sistema para excluir o PSD e não carregá-lo após a reinicialização.	Solução: Na reinicialização seguinte, a emulação não consegue carregar e o usuário pode excluir a emulação de PDS anterior e criar um novo PSD.
Un erro interno foi detectado ao restaurar a partir do arquivo de backup automático.	Se o usuário • clicar na opção **Restaurar sob backup** do Embedded Security no HPPTSM para restaurar a partir de um arquivo de backup automático • seleciona **SPSystemBackup.xml** o assistente de restauração falha e a seguinte mensagem de erro é exibida: **O arquivo de backup selecione não corresponde ao motiva da restauração. Selecione outro arquivo para continuar.**	Se o usuário seleciona **SpSystemBackup.xml** quando SpBackupArchive.xml é necessário, ocorre uma falha no assistente do Embedded Security com: **Um erro interno do Embedded Security foi detectado.** O usuário deve selecionar o arquivo .xml correto que corresponda ao motivo necessário. Os processos estão operando conforme projetado e funcionam corretamente; entretanto, a mensagem de erro interno do Embedded Security não é clara e deveria conter uma mensagem mais apropriada. A HP está trabalhando para otimizar isso em produtos futuros.
O sistema de segurança exibe um erro de restauração com múltiplos usuários.	Durante o processo de restauração, se o administrador selecionar usuários para restaurar, os usuários não selecionados não poderão restaurar as chaves ao tentar restaurar mais tarde. Uma mensagem de erro **falha no processo de decodificação** é exibida.	Os usuarios não-selecionados podem ser restaurados, restaurando o TPM, executando o processo de restauração e selecionando todos os usuários antes das próximas execuções padrão diárias de backup. Se o backup automático for executado, ele sobregrava os usuários não-restaurados e seus dados são perdidos. Se um novo backup de sistema for armazenado, os usuários previamente não-selecionados não poderão ser restaurados. Adicionalmente, o usuário deve restaurar todo o backup de sistema. Um arquivo de backup pode ser restaurado individualmente.
Restauração da memória ROM de sistema com as configurações padrão oculta o TPM.	A restauração da ROM do sistema com os valores padrão faz com que o TPM fique oculto para o Windows. Isso impede que o software de segurança opere corretamente e torna os dados criptografados por TPM inacessíveis.	Exibir o TPM no BIOS: Abra o utilitário de configuração (F10), navegue até **Segurança** > **Segurança de dispositivo**, modifique o campo de **Oculto** para **Disponível**.
O backup automático não funciona com a unidade mapeada.	Quando um administrador define o backup automático no Embedded Security, o programa cria uma entrada em **Windows** > **Tasks** > **Scheduled Task**. Esta tarefa agendada do Windows é definida para utilizar NT AUTHORITY \SYSTEM para direitos para executar o bakcup. Ela funciona corretamente em qualquer unidade local. Quando o administrador, em vez de configurar o backup automático para salvar em uma unidade de disco mapeada, o processo falha, pois NT AUTHORITY\SYSTEM não possui os direitos para utilizar a unidade mapeada.	A solução é alterar o NT AUTHORITY\SYSTEM para (nome do computador)\(nome do administrador) Esta é a configuração padrão, se a tarefa agendada for criada manualmente. A HP está trabalhando para oferecer versões futuras do produto com configurações padrão que incluam nome do computador\nome do administrador.

Descrição resumida	Detalhes	Solução
	Se o backup automático for programado para ocorrer no login, o ícone Embedded Security TNA exibe a seguinte mensagem: **O local do arquivo de backup atual não pode ser acessado. Clique a2qui se deseja fazer o backup em um arquivo temporário até que o arquivo de backup esteja acessível.** Se o backup automático for programado para um horário específico, o backup falha em exibir o aviso de falha.	
Não é possível desativar temporariamente o sstado do Embedded Security na GUI do Embedded Security.	O software 4.0 atual foi criado para implementações HP Notebook 1.1B, bem como para oferecer suporte às implementações HP Desktop 1.2. Esta opção para desativar ainda é oferecida na interface de software das plataformas TPM 1.1.	A HP corrigirá este problema em uma versão futura.

Diversos

Impactado por software – Descrição resumida	Detalhes	Solução
HP ProtectTools Security Manager—Aviso recebido: **O aplicativo de segurança não pode ser instalado até que o HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools) seja instalado**.	Todos os aplicativos de segurança, como o Embedded Security, Java Card e dados biométricos são plug-ins expansíveis da interface do HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools). O HP Security Manager deve estar instalado antes que um plug-in de segurança aprovado pela HP possa ser carregado.	O software HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools) deve estar instalado antes de instalar um plug-in de segurança.
O utilitário de autlização de firmware TPM HP ProtectTools para os modelos dc7600 e modelos contendo a TPMs ativados por Broadcom – A ferramenta fornecida pelo web site de suporte da HP reporta**propriedade obrigatória**.	Este é um comportamento esperado do utilitário de firmware TPM para os modelos dc7600 e modelos contendo TPMs ativados por Broadcom. A ferramenta de atualização de firmware permite ao usuário atualizar o firmware, com ou sem uma chave de endosso (EK). Quando não há uma chave de endossos, não é preciso autorização para completar a atualização de firmware. Quando há uma chave de endossos, é preciso haver um proprietário TPM, uma vez que o upgrade exige a autorização do proprietário. Depois de atualizar, a plataforma deve ser reiniciada para que o novo firmware entre em vigor. Se o TPM do BIOS for restaurado com os valores de fábrica, a propriedade é removida e a capacidade de atualização de firmware é bloqueada até que a plataforma de software Embedded Security e o assistente de inicialização de usuário tenham sido configurados. * A reinicialização é sempre recomendada após realizar uma atualização de firmware. A versão de firmware não é corretamente identificada até a próxima reinicialização.	1. Reinstale o software HP ProtectTools Embedded Security 2. Execute o assistente de plataforma e configuração de usuário. 3. Certifique-se para que o sistema contenha a instalação do Microsoft . NET framework 1.1: **a.** Clique em **Iniciar**. **b.** Clique em **Painel de controle**. **c.** Clique em **Adicionar ou remover programas**. **d.** Verifique se **Microsoft .NET Framework 1.1** consta na lista. 4. Verifique a configuração de hardware e software: **a.** Clique em **Iniciar**. **b.** Clique em **Todos os programas**. **c.** Clique em **HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools)**. **d.** Selecione **Embedded Security** do menu hierárquico. **e.** Clique em **Mais detalhes**. O sistema deve ter a seguinte configuração: • Versão de produto = V4.0.1 • Estado de embedded security: estado do chip = ativado, estado de propriedade = inicializado, estado de usuário = inicializado • Informação dos componentes: Versão Spec. TCG = 1.2 • Fornecedor= Broadcom Corporation

Impactado por software – Descrição resumida	Detalhes	Solução
		• Versão de FW = 2.19 (ou posterior) • Versão de biblioteca de drivers de dispositivo TPM 2.0.0.9 (ou posterior) 5. Se a versão FW não for 2.18, faça o download e atualize o firmware TPM. O TPM Firmware SoftPaq é um download de suporte disponível em http://www.hp.com.
HP ProtectTools Security Manager—Intermitente, um erro é exibido ao fechar a interface do Security Manager.	Intermitente (1 em 12 instâncias), um erro é gerado ao utilizar o botão fechar no canto superior direito da tela, para fechar o Security Manager antes que todos os aplicativos de plug-ins tenham sido totalmente carregados.	Isso está relacionado a uma dependência de sincronização no tempo de carregamento de serviços do plug-in, ao fechar e reiniciar o Security Manager. Sendo PTHOST.exe uma carcaça (shell) que comporta outros aplicativos (plug-ins), ela depende da capacidade do plug-in em completar seu tempo de carregamento (serviços). A causa do problema é o ato de fechar a carcaça antes que o plug-in tenha sido completamente carregado. Permita que o Security Manager complete a mensagem de carregamento de serviços (veja na parte superior da janela do Security Manager) e todos os plug-ins apresentados na coluna esquerda. Para evitar falhas, permita um tempo razoável para o carregamento destes plug-ins.
O acesso irrestrito geral ou privilégios de admin não-controlados do HP ProtectTools * representam um risco de segurança.	Vários riscos são possíveis com o acesso irrestrito ao computador cliente: • exclusão do PSD • modificação mal intencionada de configurações de usuário. • desativação de políticas e funções de segurança	Os administradores são encorajados a seguir as “melhores práticas” para restringir os privilégios de usuários-finais e restringir o acesso de usuários. Usuários não-autorizados não devem possuir privilégios administrativos.
A senha de sistema operacional e BIOS do Embedded Security estão fora de sincronia.	Se o usuário não validar uma nova senha como a senha de BIOS do Embedded Security, a senha de BIOS do Embedded Security volta a ser a senha original de embedded security por meio do BIOS F10.	Este recurso está funcionando corretamente; as senhas podem ser re-sincronizadas mudando a senha básica de usuário do sistema operacional e autenticando-a no prompt de senha de BIOS Embedded Security.
Apenas um usuário pode acessar o sistema depois que a autenticação pré-inicialização TPM for ativada no BIOS.	O PIN do BIOS TPM está associado ao primeiro usuário que inicializa a configuração de usuário. Se um computador possuir múltiplos usuários, o primeiro usuário é, essencialmente, o administrador. O primeiro usuário deverá fornecer seu PIN de usuário TPM aos outros usuários para que utilizem ao acessar.	Este recurso está funcionando conforme planejado; a HP recomenda que o departamento de TI do cliente siga as boas práticas de segurança para implementar sua solução de segurança e garantir que a senha de administrador do BIOS seja configurada por administradores de TI com proteção de nível de sistema.
O usuário precisa alterar o PIN para que a pré-inicialização TPM funcione após uma restauração de fábrica do TPM.	O usuário precisa alterar o PIN ou criar outro usuário para inicializar sua configuração de usuário, e ativar a autenticação de BIOS TPM após a restauração. Não há uma opção para fazer funcionar a autenticação do BIOS TPM.	Conforme planejado, a restauração de fábrica apaga a chave básica de usuário. O usuário deve alterar seu PIN ou criar um novo usuário para reiniciar a chave básica de usuário.

Impactado por software – Descrição resumida	Detalhes	Solução
O **Suporte à autenticação na ativação** não definido como padrão utilizando a **Restauração das configurações de fábrica** Embedded Security	No utilitário de configuração a opção **Suporte à autenticação na ativação** não foi restaurada com as configurações de fábrica ao utilizar a opção de dispositivo Embedded Security **Restauração das configurações de fábrica**. Por padrão, o **suporte para autenticação na ativação** é definido como **Desativado**.	A opção **Suporte à autenticação na ativação** desativa o dispositivo Embedded Security, que por sua vez, oculta outras opções do Embedded Security (incluindo a **Restauração das configurações de fábrica**). Entretanto, ao reativar o dispositivo Embedded Security, a opção **Suporte para autenticação na ativação** permanece ativa. A HP está trabalhando em uma resolução, que será fornecida em ofertas futuras de SOftwPaq ROM com base na Web
A autenticação de segurança na ativação anula a senha de BIOS durante a seqüência de inicialização.	A autenticação na ativação pede ao usuário que faça o logon no sistema utilizando a senha TPM, porém, se o usuário pressionar F10 para acessar a BIOS, obtém acessos de somente leitura.	Para poder gravar no BIOS, o usuário deve digitar a senha de BIOS em vez de senha TPM na janela de autenticação na ativação.
A BIOS pede tanto a senha nova como a antiga durante a configuração do computador após alterar a senha do proprietário no software Embedded Security Windows.	A BIOS pede tanto a senha nova como a antiga durante a configuração do computador após alterar a senha do proprietário no software Embedded Security Windows.	Esta foi uma decisão de projeto. Isso ocorre por causa da inabilidade do BIOS em se comunicar com o TPM, uma vez que o sistema operacional está em execução e para verificar a frase-senha TPM comparando-a com o arquivo blob de chave TPM.

Glossário

Acesso único (Single Sign On) Recurso que armazena dados de autenticação e permite utilizar o Credential Manager para acessar aplicativos da Internet e do Windows que exigem autenticação por senha.

Advanced Encryption Standard (AES) Uma técnica de criptografia de dados por blocos simétricos de 120 bits.

Application Programming Interface (API) Uma série de funções de sistema operacional que os aplicativos podem utilizar para realizar várias tarefas.

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

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

Autenticação Processo de verificação para autorizar um usuário a realizar uma tarefa, por exemplo, acessar um computador, modificar configurações de determinado programa, ou visualizar dados protegidos.

Autenticação na ativação Recurso de segurança que requer algumas formas de autenticação, como um Java Card, chip de segurança ou senha, quando o computador é ligado.

Autoridade certificadora Serviço que emite certificados necessários para executar uma infra-estrutura de chave pública.

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

Chip embedded security do módulo (apenas em modelos selecionados) Chip de segurança integrado que pode proteger informações de usuário sensíveis contra invasores mal-intencionados. É a raiz de confiabilidade em determinada plataforma. O TPM oferece algoritmos e operações criptográficos que atendem às especificações do TCG. O hardware e software TPM aumentam a segurança do EFS e do Personal Secure Drive, protegendo as chaves utilizadas pelo EFS e pelo PSD. Em sistemas sem o TPM, as chaves utilizadas para o EFS e PSD geralmente são armazenadas na unidade de disco rígido. Isso as torna potencialmente vulneráveis. Em sistemas com cartão TPM, as chaves de raiz de armazenamento privada do TPM, que nunca deixam o chip TPM, são utilizadas para “amarrar” ou proteger as chaves utilizadas pelo EFS e pelo PSD. Invadir um TPM para extrair chaves privadas é muito mais difícil do que invadir o disco rígido de um sistema par obtê-las. O TPM também melhora a segurança de email seguro via S/MIME no Microsoft Outlook e Outlook Express. O TPM atua como um prestador de serviços criptográficos (CSP) As chaves e certificados são geradas e/ou admitidas pelo hardware TPM, oferecem mais segurança do que implementações apenas com software.

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

Conta de rede Conta de usuário ou administrador Windows, seja em um computador local, em um grupo de trabalho ou em um domínio.

Conta de usuário do Windows Perfil de um indivíduo autorizado a acessar uma rede ou um computador individual.

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

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

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

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

Domínio Grupo de computadores que fazem parte de uma rede e compartilham de um banco de dados de diretórios comum. Os domínios possuem nomes exclusivos, e cada um possuem um conjunto de regras e procedimentos.

Identidade No ProtectTools Credential Manager, um grupo de credenciais e configurações que são utilizadas como uma conta ou perfil para um determinado usário.

Java Card Pequenas peças de hardware, similares a um cartão de crédito em tamanho e formato, que armazena informações identificáveis sobre o proprietário. Utilizado para autenticar o proprietário de um computador.

Low Pin Count (LPC) Define uma interface utilizada pelo dispositivo do HP ProtectTools Embedded Security para conectar-se ao chipset da plataforma. O barramento consiste em 4 bits de pinos de endereço/dados, junto com um clock de 33 Mhz e diversos pinos de controle/status.

Microsoft Cryptographic API, ou CryptoAPI (MSCAPI) Uma API da Microsoft que oferece uma interface ao sistema operacional Windows para aplicativos criptográficos

Migração Uma tarefa que permite gerenciar, restaurar e transferir chaves e certificados.

Modo de segurança do BIOS Configuração do Java Card Security for ProtectTools que, quando ativada, exige a utilização de um Java Card e um PIN válido para autenticação do usuário

Perfil do BIOS Grupo de definições da que podem ser salvas e aplicadas em outras contas.

Prestadores de serviços de criptografia (CSP) Prestador ou biblioteca de algoritmos criptográficos que podem ser utilizados em uma interface bem definida para realizar determinadas funções criptográficas. Um componente de software que faz interface com o MSCAPI

Public Key Cryptographic Standards (PKCS) Padrões gerados que regem a definição e utilização dos meios de codificação e decodificação de chave pública/chave privada.

Public Key Infrastructure (PKI) Um termo geral que define a implementação de sistemas de segurança que utilizam a codificação e decodificação de chave pública/chave privada.

Reinicialização Processo de reiniciar o computador.

Secure Multipurpose Internet Mail Extensions (S/MIME) Uma especificação para o envio seguro de mensagens eletrônicas utilizando o PKCS. O S/MIME oferece a autenticação via assinaturas digitais e privacidade via criptografia.

Segurança restrita Recurso de segurança na configuração do BIOS que oferece maior proteção para senhas de ativação e de administrador e outras formas de autenticação na ativação.

Senha de administrador de Java Card Senha que vincula um Java Card de administrador ao computador no utilitário de configuração para a identificação na inicialização ou reinicialização. Esta senha pode ser definida manualmente pelo administrador ou gerada aleatoriamente.

Senha de usuário de Java Card Senha que vincula um Java Card de usuário ao computador no utilitário de configuração para a identificação na inicialização ou reinicialização. Esta senha pode ser definida manualmente pelo administrador ou gerada aleatoriamente.

Sistema de arquivos criptografados (EFS) Sistema de codifica todos os arquivos e sub-pastas dentro do diretório selecionado. Um serviço de criptografia de arquivos transparente fornecido pela Microsoft para Windows 2000 ou posterior.

TCG Software Stack (TSS) Oferece serviços que tiram total proveito do TPM, porém não exigem as mesmas proteções. Oferece uma interface de software padrão para acessar as funções TPM. Para utilizar todos os recursos do TPM, como backup de chave, migração de chave, autenticação e declaração de plataforma, os aplicativos gravam diretamente no TSS.

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

Token virtual Recurso de segurança que funciona de forma similar a um Java Card e leitor. O token é salvo na unidade de disco rígido ou no registro do Windows do computador. Ao acessar o sistema com um token virtual, o usuário deve fornecer o PIN de usuário para concluir a autenticação.

Trusted Computing Group (TCG) Associação do setor criada para promover o conceito de um “PC Confiável”. O TCG substitui o TCPA.

Trusted Computing Platform Alliance (TCPA) Trusted computing alliance; agora substituída pelo TCG

Unidade pessoal segura (PSD) Oferece uma área de armazenamento protegida para dados confidenciais. Um recurso fornecido pelo HP ProtectTools Embedded Security. Este aplicativo cria uma unidade virtual no computador do usuário que automaticamente codifica arquivos/pastas que são movidos para dentro desta unidade virtual.

Índice