

Guia de Gerenciamento de Desktops

HP Business PCs

© Copyright 2009 Hewlett-Packard Development Company, L.P. As informações aqui contidas estão sujeitas à alteração sem aviso.

Microsoft, Windows, Windows Vista e Windows 7 são marcas comerciais ou marcas comerciais registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Intel e vPro 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 de Gerenciamento de Desktops

HP Business PCs

Quarta edição: setembro de 2009

Número de peça: 581009-201

Sobre este guia

Este guia apresenta definições e instruções para utilização dos recursos de segurança e capacidade de gerenciamento, previamente instalados em alguns modelos.

- △ **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 Visão Geral de Gerenciamento de Desktop

2 Configuração Inicial e Implantação

HP Client Automation Agent	2
HP Client Manager	3

3 Remote System Installation

4 Atualizações e gerenciamento de software

HP Client Management Interface	5
Gerenciador de download do HP SoftPaq	6
HP System Software Manager	6
Gerenciador de segurança HP ProtectTools	7
HP Client Automation Edições Starter e Standard	8
HP Client Automation Edição Enterprise	8
HP Client Manager from Symantec	8
Altiris Client Management Suite	9
Catálogo de Clientes HP de Produtos SMS para o Centro de Sistema Microsoft	10
Tecnologia de Gerenciamento Remoto	10
Configuração do Intel Management Engine	11
Verdiem Surveyor	13
Notificação Pró-ativa de Alteração HP	13
Subscriber's Choice	13
Soluções descontinuadas	13

5 Flash de memória ROM

Flash Remoto da Memória ROM	14
HPQFlash	14

6 Modo de recuperação de emergência do bloco de inicialização

7 Cópia da Configuração

Cópia para um computador	17
--------------------------------	----

Cópia para vários computadores	18
Criação de um Dispositivo de Inicialização	19
Dispositivos de Mídia Flash USB Admitidas	19
Dispositivos de Mídia Flash USB Não Admitidos	20

8 Botão Liga/Desliga de Dois Estados

9 Web Site de Suporte HP

10 Padrões da indústria

11 Rastreamento e segurança de equipamentos

Segurança de Senha	29
Definição de uma senha de configuração através do Utilitário de Configuração	30
Estabelecendo uma senha de inicialização utilizando o Utilitário de Configuração	30
Inserção de uma senha de inicialização	31
Digitação da senha de configuração	31
Alteração de uma senha de inicialização ou configuração	32
Exclusão de uma senha de inicialização ou configuração	32
Caracteres delimitadores no teclado nacional	33
Limpeza de senhas	33
DriveLock	33
Utilização do DriveLock	34
Aplicativos do DriveLock	34
Sensor inteligente de tampa	35
Definição do nível de proteção do sensor inteligente de tampa	35
Bloqueio Inteligente de Tampa	35
Ativação do bloqueio inteligente de tampa	36
Desativação do bloqueio inteligente de tampa	36
Utilização da Chave à Prova de Falhas do Bloqueio Inteligente da Tampa	36
Provisão de bloqueio de cabo	37
Tecnologia de identificação de impressão digital	37
Notificação e Recuperação de Falhas	37
Sistema de proteção de unidade	37
Fonte de alimentação tolerante a picos de energia	37
Sensor térmico	38


Índice	39
---------------------	-----------

1 Visão Geral de Gerenciamento de Desktop

O HP Client Management Solutions fornece soluções com base em padrões para o gerenciamento e controle de desktop, workstations e notebooks em um ambiente de rede. A HP foi pioneira em gerenciamento de desktops em 1995, quando lançou na indústria os primeiros computadores pessoais plenamente gerenciáveis. A HP possui patentes de tecnologia com capacidade de gerenciamento. Desde então, a HP tem tomado iniciativas importantes no setor para desenvolver os padrões e infraestrutura necessários para implantar, configurar e gerenciar de forma eficiente, desktops, workstations e notebooks. A HP desenvolve seu próprio software de gerenciamento e trabalha junto com os principais fornecedores de soluções de software no setor para garantir a compatibilidade entre o HP Client Management Solutions e estes produtos. As Soluções HP Client Management são um aspecto importante de nosso amplo compromisso de fornecer a você as soluções que o auxiliam na redução do custo total de propriedade e manutenção dos PCs por todo seu ciclo de vida.

Os principais recursos do gerenciamento de desktops incluem:

- Configuração e implementação inicial
- Remote System Installation
- Atualizações e gerenciamento de software
- Flash de memória ROM
- Configuração opcional de hardware
- Rastreamento de computadores e segurança
- Notificação de falha e recuperação

 **NOTA:** O suporte para recursos específicos descritos neste guia pode variar dependendo do modelo ou da versão do software.

2 Configuração Inicial e Implantação

O computador é fornecido com uma imagem de software do sistema pré-instalada. Após um breve processo de "fragmentação" do software, o computador está pronto para ser utilizado.

Pode-se substituir a imagem de software pré-instalada por um conjunto personalizado de software de sistema e aplicativos. Existem vários métodos de distribuir uma imagem de software personalizada. Elas incluem:

- Instalação de aplicativos adicionais de software após a fragmentação da imagem de software pré-instalada.
- Utilização das ferramentas de implantação de software, como HP Client Automation Standard Edition ou HP Client Automation Enterprise Edition (com base na tecnologia Radia para substituir o software preinstalado por outro, com imagem de software personalizada).
- Utilização de um processo de cópia de discos para copiar o conteúdo de uma unidade de disco para outra.

O melhor método de implantação depende de seus processos e do ambiente de tecnologia da informação.

A configuração com base em ROM e o hardware ACPI fornecem assistência adicional para recuperação do software do sistema, gerenciamento e solução de problemas de configuração e gerenciamento de energia.

HP Client Automation Agent

O agente de gerenciamento utilizado por ambos, Edições HP Client Automation Standard e Enterprise é pré-carregado no computador. Quando instalado, permite comunicação com o console de gerenciamento HP.

Para instalar o HP Client Automation Agent:

1. Clique em **Iniciar**.
2. Clique em **Todos os programas**.
3. Clique em **Capacidade de gerenciamento HP**.
4. Clique no arquivo **HP Management Agent Readme** aplicável para o idioma que você deseja.
5. Revise e siga as instruções contidas no arquivo Leia-me para instalar o HP Client Automation Agent.

O HP Client Automation Agent é um componente principal de infraestrutura para ativar todas as soluções do HP Client Automation. Para saber mais sobre outros componentes de infraestrutura

necessários para a implantação das soluções de gerenciamento de configuração HP, visite <http://h20229.www2.hp.com/solutions/ascm/index.html>.

HP Client Manager

O HP Client Manager (HPCM) é uma solução gratuita desenvolvida pela Symantec para todos os HP business desktop, notebook, workstation e HP Blade PCs admitidos. O HPCM integra ferramentas específicas HP tais como System Software Manager, HP Instant Support Professional Edition e HP Client Management Interface para ativar um modelo centralizado para o gerenciamento, rastreamento e monitoramento de todos os hardwares HP admitidos.

O HP Client Manager 7.0 inclui uma nova Página de Portal que serve como um local único onde o administrador pode executar as seguintes tarefas de gerenciamento:

- Inventário
- Alertas
- Gerenciamento de BIOS
- Atualizações de Driver
- Execução de Varredura e Diagnósticos do HP Instant Support Health
- Execução de tarefas do Embedded Security
- Visualize a Tendência de Alerta de Integridade geral nos últimos 3-6 anos.
- Visualize a conformidade geral dos computadores admitidos com Varreduras e Diagnósticos HP Instant Support Health
- Visualize o Resumo dos Computadores HP – um relatório de vários desktops, notebooks, workstations e HP Blade PCs admitidos
- Visualize Alertas: Equipamento, Limite, Integridade de Hardware
- Relatórios
- Tarefas administrativas para atualizar ferramentas específicas HP


Pode ser feito download do HPCM a partir de <http://www.symantec.com/business/theme.jsp> clicando em **HP Client Manager** abaixo de **Strategic Partner Products** (Produtos Estratégicos de Parceiros). Uma licença permanente gratuita também pode ser obtida a partir da página de download.

Vídeos HPCM “How to” também estão publicados em <http://www.symantec.com/connect>. Pesquise em **HP Client Manager 7.0** para visualizar passo a passo os vídeos de várias tarefas com o HPCM.

3 Remote System Installation

A Instalação Remota do Sistema permite inicializar e configurar o sistema utilizando o software e as informações de configuração localizadas em um servidor de rede, ao iniciar o Ambiente de Execução antes da Inicialização (Preboot Execution Environment - PXE). O recurso de Instalação Remota do Sistema geralmente é utilizado como ferramenta de inicialização e configuração do sistema, e pode efetuar as seguintes tarefas:

- Formatação de uma unidade de disco rígido
- Implementação de imagem de software para um ou mais novos PCs
- Atualização remota do BIOS do sistema em memória flash ROM ([Flash Remoto da Memória ROM na página 14](#))

 **NOTA:** Existem instalações para flash do BIOS do sistema como sistema operacional Microsoft Windows.

- Configuração das definições do BIOS do sistema

Para iniciar a Remote System Installation, pressione **F12** enquanto a mensagem **F12 = Network Service Boot** (F12 = Inicialização por serviço da rede) é exibida no canto inferior direito da tela com o logotipo HP durante a inicialização do computador. Siga as instruções exibidas na tela para prosseguir o processo. A sequência padrão de inicialização é uma definição de configuração do BIOS que pode ser alterada sempre que se tenta uma inicialização PXE.

4 Atualizações e gerenciamento de software

A HP fornece diversas ferramentas para gerenciamento e atualização de software em desktops, workstations e notebooks:

- Interface HP Client Management
- Gerenciador de download do HP SoftPaq
- HP System Software Manager
- HP ProtectTools Security Manager
- HP Client Automation Edições Starter, Standard e Enterprise
- HP Client Manager from Symantec
- Altiris Client Management Suite
- Catálogo de Clientes HP de Produtos SMS para o Centro de Sistema Microsoft
- PCs com a marca Intel vPro com a Tecnologia de Gerenciamento de Ativo (Active Management Technology)
- Verdiem Surveyor
- HP Proactive Change Notification
- HP Subscriber's Choice

HP Client Management Interface

Independente das ferramentas de gerenciamento do sistema que seu departamento de TI utiliza, é importante gerenciar seus ativos de hardware e software, para manter baixos seus custos de TI e seu negócio ágil. O administrador de TI pode acessar a interface HP Client Management gravando scripts simples e integrando esses scripts à solução de gerenciamento de sua escolha.

Com a Interface HP Client Management (HP CMI), novos business HP integram-se perfeitamente em seu ambiente de TI gerenciado. HP CMI fornece uma interface que simplifica a integração dos HP business PCs com as ferramentas de gerenciamento de sistema populares na indústria (incluindo Microsoft Systems Management Server, IBM Tivoli Software, e HP Operations) e aplicativos de gerenciamento personalizados implantados no local. Usando o HP CMI, aplicativos e ferramentas de gerenciamento de sistemas podem solicitar inventário detalhado de cliente, receber informação de status de integridade e gerenciar as configurações do BIOS para comunicação diretamente com o computador cliente, reduzindo a necessidade do software agente ou conector para obter integração.

A HP Client Management Interface baseia-se nos padrões da indústria que inclui o Microsoft Windows Management Interface (MS WMI), Web-Based Enterprise Management (WBEM), System Management BIOS (SMBIOS) e Advanced Configuration and Power Interface (ACPI). HP CMI é uma tecnologia de base utilizada no HP Client Management Solutions. Com ele, a HP pode lhe proporcionar mais flexibilidade para escolher como administrar seus computadores clientes HP.

A HP Client Management Interface, utilizada com o software de gerenciamento de sistema pode:

- Solicitação de informação sobre inventário em profundidade de Clients — Capturar informações detalhadas sobre os processadores, unidades de disco rígido, memória BIOS, drivers, incluindo informação sobre sensores (como velocidade de ventilador, voltagem e temperatura).
- Receber informações sobre o estado de integridade — Assine diversos tipos de alertas de hardware cliente (como excesso de temperatura, parada do ventilador e alterações na configuração de hardware) para enviar para o console de gerenciamento de sistema, aplicativo ou para o computador cliente local. Os alertas são enviados em tempo real quando acionados por eventos de hardware.
- Gerenciar configurações do BIOS do sistema — Executar as funções F10 incluindo definição e alteração de senhas e seqüência de inicialização do computador de forma remota, a partir do console de gerenciamento de sistema, em um sistema específico ou todos os sistemas clientes, sem precisar visitar cada máquina.

Para obter mais informações sobre a Interface HP Client Management, consulte <http://www.hp.com/go/hpcmi/>.

Gerenciador de download do HP SoftPaq


O Gerenciador de Download do HP SoftPaq (HP SoftPaq Download Manager) é uma interface gratuita, fácil de usar para localizar e fazer download de atualizações de software para os modelos HP client PC em seu ambiente. Para especificar seus modelos, sistema operacional e idioma, você pode localizar rapidamente, escolher e selecionar os softpaqs que você necessita. Para fazer o download do HP SoftPaq Download Manager, visite <http://www.hp.com/go/sdm>.

HP System Software Manager

O HP System Software Manager (SSM) é um utilitário gratuito que automatiza a implantação remota de drivers de dispositivo e atualizações do BIOS em seus HP Business PCs conectados em rede. Quando o SSM é executado, ele anonimamente (sem interação do usuário) determina os níveis de revisão dos drivers e BIOS instaladas em cada sistema cliente e compara este inventário contra os SoftPaqs de software do sistema, que foram testados e armazenados em um depósito central de arquivos. Em seguida, o SSM atualiza automaticamente qualquer software de sistema de revisão desatualizada nos PCs em rede para níveis posteriores disponíveis no depósito de arquivos. Como o SSM permite apenas a distribuição de atualizações através de SoftPaq nos modelos de sistema de cliente corretos, os administradores podem empregar com confiança e eficiência o SSM para manter o software de sistema atualizado.

O System Software Manager é integrado às ferramentas de distribuição de software corporativo, como as soluções HP Client Automation, HP Client Manager from Symantec e Microsoft Systems Management Server (SMS). Com a utilização do SSM, você pode distribuir atualizações criadas pelo cliente ou por terceiros que foram embaladas no formato SSM.

O SSM pode ser obtido por download gratuitamente acessando <http://www.hp.com/go/ssm>.

 **NOTA:** O SSM atualmente não admite flash remoto da memória ROM em sistemas que têm o Windows BitLocker Drive Encryption ativado e estão utilizados medidas TPM para proteger as chaves BitLocker porque ao fazer flash no BIOS invalida a assinatura confiável que BitLocker criou para a plataforma. Desative BitLocker através de Critérios de Grupo para que possa fazer flash no BIOS do sistema.

Você pode ativar o suporte BitLocker sem medições TPM do BIOS para evitar invalidar as chaves BitLocker. A HP recomenda que você mantenha backup seguro das credenciais do BitLocker para caso de recuperação de emergência.

Gerenciador de segurança HP ProtectTools

O software de segurança HP ProtectTools fornece recursos de segurança que ajudam a proteger contra acesso não-autorizado ao computador, redes e dados críticos. A funcionalidade de segurança avançada é oferecida pelos seguintes módulos, e está acessível através do HP ProtectTools Security Manager:

O HP ProtectTools Security Manager é um simples console através do qual todos os outros módulos são acessados.

- Credential Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Privacy Manager for HP ProtectTools
- File Sanitizer for HP ProtectTools
- Java Card Security for HP ProtectTools
- Embedded Security for HP ProtectTools
- Device Access Manager for HP ProtectTools
- LoJack Pro for HP ProtectTools

O HP ProtectTools oferece duas versões que podem ser utilizadas: HP ProtectTools Security Manager e HP ProtectTools Administrative Console. Ambas as versões, do Administrador e do usuário estão disponíveis no menu **Iniciar > Todos os Programas**.

Os módulos de software disponíveis para seu computador podem variar de acordo com o modelo. Por exemplo, o Embedded Security for HP ProtectTools está disponível somente em computadores que possuem o chip de segurança integrada TPM (Trusted Platform Module) instalado.

Os módulos de software HP ProtectTools podem estar pré-instalados, pré-carregados ou disponíveis para download do Web site da HP. Para selecionados HP Pro Desktops, o HP ProtectTools está disponível como uma opção pós-venda. Visite <http://www.hp.com/products/security> para obter mais informações.

HP Client Automation Edições Starter e Standard

HP Client Automation é uma solução de gerenciamento de hardware e software para ambientes Windows Vista, Windows XP e HP Thin Client que é fácil de usar e rápido para implantar, enquanto fornece uma base sólida para necessidades futuras. É oferecida em duas edições:

- A Edição Starter é um produto gratuito para gerenciamento de desktops HP, notebooks e workstations, oferecendo inventário de hardware e software, controle remoto, monitoração de alertas HP, atualizações do BIOS e driver, integração com HP Protect Tools e suporte adicional para Intel AMT. A Edição Starter também dá suporte à implantação e gerenciamento do HP Thin Clients.
- A Edição Standard, disponível para aquisição, inclui toda funcionalidade fornecida na Edição Starter e adiciona implantação e migração do Windows, recursos de gerenciamento de patch, distribuição de software e medição do uso de software.

A HP Client Automation Edições Starter e Standard fornece um caminho de migração para a HP Client Automation Edição Enterprise (com base em tecnologia Radia) para gerenciamento automatizado para grandes ambientes de TI, heterogêneos e continuamente em alteração.

Para obter mais informações sobre as soluções HP Client Automation, visite <http://www.hp.com/go/client>.

HP Client Automation Edição Enterprise

A HP Client Automation Edição Enterprise é uma solução com base em critérios que ativa administradores para inventário, implantação, caminhos e gerencia continuamente software e conteúdo em plataformas clientes heterogêneas. Com a HP Client Automation Edição Enterprise, o profissional de TI pode:

- Automatizar o processo completo de gerenciamento de ciclo de vida de busca, implantação e gerenciamento contínuo através de migração e descontinuidade.
- Implantar automaticamente e gerenciar continuamente todo um conjunto de software (sistemas operacionais, aplicativos, caminhos, configurações e conteúdo) para um estado desejado.
- Gerenciar software em virtualmente todos os dispositivos, incluindo desktops, workstations e notebooks, em uma infra-estrutura heterogênea ou independente.
- Gerenciar software na maioria dos sistemas operacionais.

Com gerenciamento contínuo de configuração, os clientes HP informam economia dramática em custos de TI, tempo de colocação no mercado acelerado para software e conteúdo e uma maior produtividade e satisfação por parte dos usuários.

Para obter mais informações sobre as soluções HP Client Automation, visite <http://www.hp.com/go/client>.

HP Client Manager from Symantec

O HP Client Manager from Symantec, desenvolvido com a Altiris, está disponível gratuitamente para todos os modelos de HP business desktop, notebook e workstation admitidos. O SSM é integrado ao HP Client Manager e permite acompanhamento, monitoramento e gerenciamento centralizados dos aspectos de hardware de sistemas HP Client.

Utilize o HP Client Manager from Symantec para:

- Obter informações valiosas de hardware como CPU, memória, vídeo e configurações de segurança
- Monitorar a integridade do sistema para solucionar problemas antes que eles ocorram
- Obter e instalar automaticamente drivers e atualizações do BIOS sem visitar cada PC
- Configurar o BIOS e as configurações de segurança remotamente
- Automatizar processos para resolver problemas de hardware rapidamente

Estrita integração com as ferramentas do HP Instant Support que reduz o tempo para a solução de problemas.

- Diagnósticos — execute e visualize remotamente relatórios sobre os modelos desktop, notebook e workstation HP
- System Health Scan — verificar se há problemas de hardware em seu conjunto de sistemas clientes HP
- Active Chat — conecte-se ao suporte ao cliente HP para a resolução de problemas.
- Base de Conhecimentos HP — acesso a informações especializadas
- Processo automatizado de coleta e fornecimento de SoftPaqs para solução rápida de problemas de hardware
- Identificação, geração de relatório de estoque e inicialização de sistemas com o chip de segurança integrado HP ProtectTools.
- Opção de exibir alertas de integridade de modo local no PC
- Envio de informações básicas de inventário para clientes não-HP
- Definição e configuração do chip de segurança TPM
- Agenda centralizada de backup e recuperação de client
- Suporte para gerenciamento de AMT Intel

Para obter mais informações sobre o HP Client Manager from Symantec, visite <http://www.hp.com/go/clientmanager>.

Altiris Client Management Suite

Altiris Client Management Suite é uma solução fácil de usar para gerenciamento completo do ciclo de vida de software de desktops, notebooks e workstations. Client Management Suite inclui os seguintes produtos Altiris:

- Solução de Inventário (Inventory Solution)
- Solução de Implantação (Deployment Solution)
- Solução de Distribuição de Software (Software Delivery Solution)
- Solução de Gerenciamento de Patch (Patch Management Solution)
- Solução de Medição de Aplicativo (Application Metering Solution)

- Solução de Gerenciamento de Aplicativo (Application Management Solution)
- Solução Carbon Copy (Carbon Copy Solution)

Para obter mais informações sobre o Altiris Client Management Suite, visite <http://www.symantec.com/business/client-management-suite>.

Catálogo de Clientes HP de Produtos SMS para o Centro de Sistema Microsoft

O Catálogo de Clientes HP permite que profissionais de TI utilizem produtos Microsoft para automatizar a implantação das atualizações de software HP (Softpaqs) em HP business PCs. O arquivo do catálogo contém informações detalhadas sobre plataformas em HP business desktops, notebooks e workstations. Elas podem ser usadas em conjunto com o inventário personalizado e recursos de atualização dos produtos Microsoft para fornecer driver automatizado e atualizações de patch para computadores HP client gerenciados.

Os produtos Microsoft admitidos pelo de Clientes HP incluem:

- System Center Configuration Manager 2007
- System Center Essentials 2007
- Systems Management Server (SMS) 2003 R2

Para obter mais informações sobre o Catálogo de Clientes HP para SMS, visite <http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html>.

Tecnologia de Gerenciamento Remoto


Os modelos incluem tecnologia vPRO ou tecnologia padrão. Ambas permitem melhor descoberta, reparação e proteção de ativos computacionais da rede. Ambas as tecnologias permitem que os PCs sejam gerenciados com o sistema ligado ou desligado, ou com o sistema operacional travado.

Os três modos de capacidade de gerenciamento remoto disponíveis em business desktops são Alert Standard Format (ASF), Intel Active Management Technology (AMT), e Desktop and mobile Architecture for Systems Hardware (DASH).


Os recursos de tecnologia de gerenciamento remoto incluem:

- Descoberta de rede
- Informação de inventário de hardware
- Monitoramento da integridade da plataforma
- Gerenciamento de energia — liga/desliga, distribuição de energia
- Diagnóstico e reparo remoto
 - Redirecionamento do console de texto-permite o controle do console de PC remoto durante sua fase de inicialização.
 - Redirecionamento de mídia-permite ao sistema inicializar a partir de uma unidade, disco ou imagem ISO de inicialização remota (as duas variantes disso são IDE-Redirect (IDE-R) em plataformas AMT e USB Media Redirection)

- Isolamento e recuperação com base em hardware — limita ou interrompe o acesso à rede do PC, em caso de detecção de padrão de atividade de vírus
- Rastreamento e auditoria de eventos na plataforma
- Portal de gerenciamento de servidor web integrado para acesso e configuração remota
- As tecnologias de gerenciamento remoto são integradas com console de gerenciamento de parceiros da HP

 **NOTA:** Nem todos os recursos acima estão disponíveis em todas as plataformas.

Configuração do Intel Management Engine

 **NOTA:** Para obter uma visão geral da tecnologia Intel vPro, visite <http://www.intel.com/vpro>.

Para obter informação específica da HP sobre a tecnologia Intel vPro, consulte a documentação técnica em <http://www.hp.com.br/suporte>. Selecione seu país e idioma **Ver informações sobre suporte e solução de problemas**, digite o número do modelo do computador, e pressione **Enter**. Na categoria **Resources** (Recursos), clique em **Manuals (guides, supplements, addendums, etc.)** (Manuais (guias, suplementos, adendos, etc.)). Em **Introdução rápida aos manuais por categoria**, clique em **Documentos técnicos**.


As tecnologias de gerenciamento disponíveis incluem o seguinte:

- AMT (inclui DASH 1.0)
- ASF
- DASH 1.1 (usando uma NIC Broadcom)

ASF e AMT não podem ser configurados simultaneamente, porém são admitidos.

Para configurar sistemas Intel vPro para o AMT ou ASF:

1. Ligue ou reinicie o computador. Se estiver no Microsoft Windows, clique em **Iniciar > Desligar > Reiniciar**.
2. Assim que o computador é ligado, pressione a tecla fr atalho, **Ctrl+p**, antes que o computador inicie o sistema operacional.

 **NOTA:** Se você não pressionar **Ctrl+p** no momento apropriado, você terá que reiniciar o computador e pressionar novamente **Ctrl+p** antes que o computador inicie o sistema operacional para acessar o utilitário.

Esta tecla de atalho leva ao utilitário de configuração Intel Management Engine BIOS Execution (MEBx). Este utilitário permite que o usuário configure os vários aspectos da tecnologia de gerenciamento. Algumas das opções de configuração estão listadas abaixo:

- Menu Principal
 - Configuração Intel® ME
 - Configuração Intel® AMT
 - Alteração da Senha do Intel® ME
 - Sair
- Configuração da Plataforma Intel® ME
 - Controle do Estado do Intel® ME (ativado/desativado)
 - Atualização Local de Firmware do Intel® ME (ativado/desativado)
 - Controle dos Recursos do Intel® ME
 - Controle de Energia do Intel® ME
- Configuração Intel® AMT
 - Nome do Host
 - TCP/IP
 - Modelo de Provisão (Enterprise, SMB)
 - Instalação e Configuração
 - Sem Provisão
 - SOL/IDE-R (ativar/desativar)
 - Política de Senha
 - Atualização de Segurança de Firmware (ativar/desativar)
 - Configuração de PRTC
 - Tempo Limite de Inatividade
- Alteração de Senha do Intel® ME (A HP recomenda altamente que esta senha seja alterada. A configuração padrão é **admin**.)

Para gerenciar remotamente sistemas AMT, o administrador deve utilizar um console remoto que admita AMT. Consoles de gerenciamento corporativo estão disponíveis para fornecedores como HP, Altiris and Microsoft SMS. No modo SMB, o cliente oferece uma interface de navegador Web. Para acessar esse recurso, abra um navegador a partir de qualquer outro sistema na rede e digite `http://host_name:16992` onde `host_name` é o nome designado para o sistema. Alternativamente, o endereço IP pode ser utilizado em lugar do nome host.

Para configurar o sistema com uma NIC apta para Broadcom DASH:

Verifique a documentação mais recente no site <http://www.hp.com.br> abaixo de **Suporte e Solução de Problemas**, em seguida selecione seu modelo específico, e selecione **Manuais**, depois **Documentos técnicos** referentes a DASH ou à NIC Broadcom.

Verdiem Surveyor

Verdiem Surveyor é uma solução de software que ajuda gerenciar custos de energia do PC. Surveyor mede e relata quanto cada PC consome de energia. Ele também fornece controle sobre as configurações de energia do PC permitindo que os administradores implantem facilmente de estratégias para economia de energia em todas suas redes. Um HP SoftPak contendo o agente Surveyor pode fazer download a partir do site de Suporte HP e instalar em modelos de desktop comercial que admitem. Licenças Surveyor para gerenciamento de PCs podem ser adquiridas através de seu representante HP.

Notificação Pró-ativa de Alteração HP

O programa Notificação pró-ativa de alteração usa o Web site do Subscriber's Choice de forma pró-ativa e automática para:

- Enviar-lhe e-mails de Notificação pró-ativa de alteração (PCN) com informações sobre alterações de hardware ou software na maioria dos computadores e servidores comerciais, com até 60 dias de antecedência.
- Enviar e-mails contendo boletins ao cliente, conselhos ao cliente, notas ao cliente, boletins de segurança e alertas de Drivers para a maioria dos computadores e servidores comerciais

Crie seu próprio perfil para garantir que receba apenas as informações relevantes para um determinado ambiente de TI. Para obter mais informações sobre o programa de Notificação Pró-ativa de Alteração e criar um perfil personalizado, visite <http://h30046.www3.hp.com/subhub.php>

Subscriber's Choice

O Subscriber's Choice é um serviço com base no cliente da HP.

Com base em seu perfil, a HP lhe fornecerá dicas personalizadas sobre produtos, divulgações e/ou notificações/alertas sobre drivers e suporte.

As Notificações/Alertas de Drivers e Suporte da Seleção do Assinante enviarão e-mails comunicando-o que as informações às quais foram definidas em seu perfil estão disponíveis para revisão e download. Para saber mais sobre Subscriber's Choice (seleção de assinante) e criar um perfil personalizado, visite <http://h30046.www3.hp.com/subhub.php>.

Soluções descontinuadas

Dois pacotes de software, Altiris Local Recovery e Dantz Retrospect, já não poderão ser enviados em HP business desktops, notebooks ou workstations.

5 Flash de memória ROM

O BIOS do computador é armazenado em uma memória ROM (memória somente de leitura) flash programável. Ao definir uma senha de configuração no Utilitário de Configuração (F10) do Computador, é possível proteger a memória ROM de atualização ou gravação não-proposital. Isso é importante para garantir a integridade da operação do computador. Se houver necessidade ou desejo de atualizar o BIOS, você pode fazer download das imagens mais recentes do BIOS a partir da página de suporte e driver HP, <http://www.hp.com.br/suporte/arquivos>.

- △ **CUIDADO:** Para proteção máxima da memória ROM, assegure-se de estabelecer uma senha de configuração. A senha de configuração impede atualizações não autorizadas da memória ROM. O gerenciador de software do sistema permite ao administrador do sistema definir a senha de configuração em um ou mais PCs simultaneamente. Para obter mais informações, visite <http://www.hp.com/go/ssm>.

Flash Remoto da Memória ROM

O Flash de memória ROM remoto permite ao administrador do sistema atualizar com segurança a memória ROM em computadores HP remotos diretamente do console de gerenciamento centralizado da rede. A ativação do administrador de sistema para realizar esta tarefa remotamente em múltiplos computadores resulta em uma implementação consistente e de maior controle sobre imagens HP PC BIOS através da rede. Isso também resulta em maior produtividade e menor custo total de propriedade.

- 📅 **NOTA:** O SSM atualmente não admite flash remoto da memória ROM em sistemas que têm o Windows BitLocker Drive Encryption ativado e estão utilizados medidas TPM para proteger as chaves BitLocker porque ao fazer flash no BIOS invalida a assinatura confiável que BitLocker criou para a plataforma. Desative BitLocker através de Critérios de Grupo para que possa fazer flash no BIOS do sistema.

O computador deve estar ligado, ou ser ligado por Restauração remoto, para ser possível utilizar o Flash da memória ROM remoto.

Para obter maiores informações sobre o flash remoto da memória ROM, consulte o Software HP Client Manager ou o System Software Manager em <http://www.hp.com/go/ssm>.

HPQFlash

O utilitário HPQFlash é utilizado para atualizar ou restaurar localmente o BIOS do sistema em PCs através do sistema operacional Windows.

Para obter mais informações sobre o HPQFlash, visite <http://www.hp.com.br/suporte/arquivos> e digite o número do modelo do computador quando solicitado.

6 Modo de recuperação de emergência do bloco de inicialização


O Modo de Recuperação de emergência do bloco de inicialização permite recuperação do sistema no caso improvável de uma falha da memória ROM flash. Por exemplo, se ocorresse uma falha de energia durante uma atualização de BIOS, a memória ROM flash ficaria incompleta. Isto provocaria a inutilização do BIOS de sistema. O Boot Block é uma seção protegida por flash da ROM contendo código que verifica a validade da imagem do BIOS de sistema quando o sistema é ativado.

- Se a memória ROM do sistema for válida, o sistema se inicializa normalmente.
- Se a imagem do BIOS de sistema não for válida, um BIOS com bloqueio de inicialização à prova de falhas oferecerá suficiente suporte para pesquisar arquivos de imagem de BIOS em mídia removível. Se um arquivo de imagem do BIOS apropriado for encontrado, ele será protegido automaticamente na memória ROM.

Quando uma imagem de BIOS de sistema inválida for detectada, o LED de alimentação de sistema piscará 8 vezes na cor vermelha, uma piscada a cada segundo. Simultaneamente, o alto-falante soará 8 vezes. Se a parte da memória ROM de sistema contendo a imagem de memória ROM com opção de vídeo não estiver corrompida, **Boot Block Emergency Recovery Mode** (Modo de recuperação de emergência do bloco de inicialização) será exibido na tela.

Para recuperar o sistema após ter entrado no Modo de recuperação de emergência do bloco de inicialização, siga as seguintes etapas:

1. Desligue a energia.
2. Insira um CD ou dispositivo flash USB contendo o arquivo de imagem do BIOS desejado no diretório raiz.


 **NOTA:** A mídia deve ser formatada utilizando o sistema de arquivos FAT12, FAT16 ou FAT32.

3. Ligue o computador.

Se nenhuma imagem do BIOS apropriado for encontrada, você será solicitado a inserir a mídia contendo um arquivo de imagem do BIOS.


Se o sistema reprogramar a memória ROM com sucesso, o sistema será desligado automaticamente.

4. Retire a mídia removível utilizada para atualizar o BIOS.
5. Ligue-o novamente para reiniciar.

 **NOTA:** O BitLocker evita a inicialização a partir do Windows Vista quando um CD contendo o arquivo de imagem do BIOS é inserido na unidade óptica. Se o BitLocker é ativado, remova este CD antes de tentar iniciar com o Windows Vista.

7 Cópia da Configuração

Os procedimentos a seguir permitem ao administrador copiar facilmente uma configuração de inicialização para outros computadores do mesmo modelo. Isso permite a configuração mais rápida e consistente de vários computadores.


 **NOTA:** Ambos os procedimentos exigem uma unidade de disquete ou uma unidade flash USB admitida.

NOTA: O System Software Manager (SSM) pode ser usado para replicar informação de configuração do computador com o sistema operacional Windows. Para obter mais informações consulte o Guia do Usuário do SSM em <http://www.hp.com/go/ssm>.

Cópia para um computador

△ **CUIDADO:** A definição de configuração depende do modelo. O sistema de arquivos pode ser corrompido se os computadores de origem e destino não forem do mesmo modelo. Por exemplo, não copie a configuração estabelecida a partir de um PC dc7xxx para um PC dx7xxx.

1. Selecione a definição de configuração para copiar. Desligue o computador. Se estiver no Windows, clique em **Iniciar > Desligar > Desligar**.
2. Se estiver utilizando um dispositivo de mídia flash USB, insira-o agora.
3. Ligue o computador.
4. Assim que o computador estiver ligado, pressione **F10** antes que o computador inicie o sistema operacional para entrar no utilitário de configuração. Pressione **Enter** para omitir a tela de abertura, se necessário.

 **NOTA:** Se a tecla **F10** não for pressionada no momento certo, você deverá reiniciar o computador e pressionar novamente **F10** antes que o computador inicie o sistema operacional para acessar o utilitário.

5. Se estiver usando um disquete, insira-o agora.
6. Clique em **File (Arquivo) > Replicated Setup (Configuração replicada) > Save to Removable Media (Salvar para mídia removível)**. Siga as instruções na tela para criar o disquete ou dispositivo de mídia flash USB de configuração.
7. Desligue o computador a ser configurado e insira o disquete ou dispositivo de mídia flash USB de configuração.
8. Ligue o computador a ser configurado.

- Assim que o computador estiver ligado, pressione **F10** antes que o computador inicialize o sistema operacional para entrar no utilitário de configuração. Pressione **Enter** para omitir a tela de abertura, se necessário.
- Clique em **File** (Arquivo) > **Replicated Setup** (Configuração replicada) > **Restore from Removable Media** (Restaurar a partir de mídia removível), e siga as instruções na tela.
- Reinicie o computador após concluir a configuração.

Cópia para vários computadores

△ **CUIDADO:** A definição de configuração depende do modelo. O sistema de arquivos pode ser corrompido se os computadores de origem e destino não forem do mesmo modelo. Por exemplo, não copie a configuração estabelecida a partir de um PC dc7xxx para um PC dx7xxx.

Este método demora um pouco mais para preparar o disquete ou dispositivo de mídia flash USB de configuração, mas copiar a configuração para os computadores de destino é bem mais rápido.

✍ **NOTA:** Um disquete de inicialização é necessário para este procedimento ou para criar um dispositivo de inicialização de mídia flash USB. Se não houver um Windows XP disponível para criar um disquete de inicialização, use o método de copiar para um computador (consulte [Cópia para um computador na página 17](#)).

- Crie um disquete ou dispositivo de mídia flash USB de inicialização. Consulte [Dispositivos de Mídia Flash USB Admitidas na página 19](#) ou [Dispositivos de Mídia Flash USB Não Admitidos na página 20](#).

△ **CUIDADO:** Nem todos os computadores podem ser inicializados por dispositivo de mídia Flash USB. Se a ordem padrão de inicialização no Utilitário de Configuração (F10) do computador relaciona o dispositivo USB antes da unidade de disco rígido, é possível inicializar o computador de um dispositivo de mídia flash USB. Caso contrário, deve ser utilizado um disquete de inicialização.

- Selecione a definição de configuração para copiar. Desligue o computador. Se estiver no Windows, clique em **Iniciar** > **Desligar** > **Desligar**.
- Se estiver utilizando um dispositivo de mídia flash USB, insira-o agora.
- Ligue o computador.
- Assim que o computador estiver ligado, pressione **F10** antes que o computador inicialize o sistema operacional para entrar no utilitário de configuração. Pressione **Enter** para omitir a tela de abertura, se necessário.

✍ **NOTA:** Se a tecla **F10** não for pressionada no momento certo, você deverá reiniciar o computador e pressionar novamente **F10** antes que o computador inicialize o sistema operacional para acessar o utilitário.

- Se estiver usando um disquete, insira-o agora.
- Clique em **File** (Arquivo) > **Replicated Setup** (Configuração replicada) > **Save to Removable Media** (Salvar para mídia removível). Siga as instruções na tela para criar o disquete ou dispositivo de mídia flash USB de configuração.
- Faça o download do utilitário do BIOS para replicar a configuração (repset.exe) e copie-o para o disquete ou dispositivo de mídia flash USB de configuração. Para obter este utilitário, visite <http://welcome.hp.com/country/us/en/support.html> e digite o número do modelo do computador.

9. No disquete ou dispositivo de mídia flash USB de configuração, crie um arquivo autoexec.bat contendo o seguinte comando:

```
repset.exe
```

10. Desligue o computador a ser configurado. Insira o disquete ou dispositivo de mídia flash USB de configuração e ligue o computador. O Utilitário de Configuração é executado automaticamente.
11. Reinicie o computador após concluir a configuração.

Criação de um Dispositivo de Inicialização

Dispositivos de Mídia Flash USB Admitidas

Dispositivos admitidos possuem uma imagem pré-instalada para simplificar o processo de torná-los inicializáveis. Todos os dispositivos de mídia flash USB HP ou Compaq e a maioria dos outros dispositivos do mesmo tipo possuem esta imagem pré-instalada. Se o dispositivo de mídia flash USB em uso não tiver essa imagem, use o procedimento descrito mais adiante nesta seção (consulte [Dispositivos de Mídia Flash USB Não Admitidos na página 20](#)).

Para criar um dispositivo de mídia flash USB de inicialização, é necessário ter:

- um dispositivo de mídia flash USB admitido
- um disquete DOS inicializável com os programas FDISK e SYS (se SYS não estiver disponível, FORMAT poderá ser utilizado, porém, todos os arquivos existentes no dispositivo de mídia flash USB serão perdidos.)
- um PC inicializável a partir de um dispositivo de mídia flash USB

△ **CAUIDADO:** Alguns PCs mais antigos podem não ser inicializados a partir de um dispositivo de mídia flash USB. Se a ordem padrão de inicialização no Utilitário de Configuração (F10) do computador relaciona o dispositivo USB antes da unidade de disco rígido, é possível inicializar o computador de um dispositivo de mídia flash USB. Caso contrário, deve ser utilizado um disquete de inicialização.

1. Desligue o computador.
2. Insira o dispositivo de mídia Flash USB em uma das portas USB do computador e remova todos os demais dispositivos de armazenamento USB, exceto as unidades de disquete USB.
3. Insira um disquete DOS de inicialização com FDISK.COM e também SYS.COM ou FORMAT.COM, em uma unidade de disquete e ligue o computador para inicializar a partir do disquete DOS.
4. Execute FDISK a partir da solicitação **A:** digitando **FDISK** e pressionando **Enter**. Se for solicitado, clique em **Sim (S)** para ativar o suporte a discos de grande capacidade.
5. Entre na opção [5] para exibir as unidades no sistema. O dispositivo de mídia flash USB será a unidade que se aproxima mais do tamanho de uma das unidades relacionadas. Geralmente é a última unidade na relação. Observe a letra da unidade.

Unidade do dispositivo de mídia flash USB: _____

△ **CUIDADO:** Se nenhuma unidade corresponde ao dispositivo de mídia flash USB, não prossiga. Pode-se perder dados. Verifique se não há dispositivos de armazenamento em outras portas USB. Se encontrar algum, remova-os, reinicialize o computador e proceda à etapa 4. Se não encontrar nenhum, o sistema não é compatível com o dispositivo de mídia flash USB ou está com defeito. NÃO prossiga tentando tornar o dispositivo de mídia flash USB de inicialização.

6. Saia de FDISK ao pressionar a tecla **Esc** para voltar ao prompt **A:**.
7. Se o disquete DOS de inicialização contém o arquivo SYS.COM, vá para a etapa 8. Opcionalmente, vá para a etapa 9.
8. No prompt **A:** digite `SYS x:` onde x representa a letra da unidade indicada acima.

△ **CUIDADO:** Assegure-se de que digitou a letra correta de unidade para o dispositivo de mídia flash USB.


Após transferir os arquivos de sistema, SYS retorna ao prompt **A:**. Vá para a etapa 13.

9. Copie quaisquer arquivos que deseja manter do dispositivo de mídia flash USB para um diretório temporário em outra unidade de disco (por exemplo, unidade de disco rígido interno do sistema).
10. No prompt **A:** digite `FORMAT /S X:` onde X representa a letra da unidade indicada anteriormente.

△ **CUIDADO:** Assegure-se de que digitou a letra correta de unidade para o dispositivo de mídia flash USB.

FORMAT exibirá uma ou mais mensagens e pergunta, a cada etapa, se você deseja continuar. Digite sempre **S**. FORMAT formatará o dispositivo de mídia flash USB, acrescentará os arquivos do sistema e pedirá um Nome para a Unidade (Volume Label).

11. Pressione **Enter** para não nomear, ou digite um, se desejar.
12. Copie os arquivos salvos na etapa 9 de volta para seu dispositivo de mídia flash USB.
13. Remova o disquete e reinicialize o computador. O computador inicializará pelo dispositivo de mídia flash USB como sendo a unidade C.

 **NOTA:** A seqüência padrão de inicialização varia de um computador para outro e pode ser alterada no Utilitário de Configuração (F10) do computador.

Se utilizou uma versão DOS do Windows 9x, poderá ser exibida rapidamente uma tela com o logotipo do Windows. Para não exibir essa tela, acrescente um arquivo de comprimento zero chamado LOGO.SYS ao diretório raiz do dispositivo de mídia flash USB.

Retorne para [Cópia para vários computadores na página 18](#).

Dispositivos de Mídia Flash USB Não Admitidos

Para criar um dispositivo de mídia flash USB de inicialização, é necessário ter:


- um dispositivo de mídia flash USB
- um disquete DOS inicializável com os programas FDISK e SYS (se SYS não estiver disponível, FORMAT poderá ser utilizado, porém, todos os arquivos existentes no dispositivo de mídia flash USB serão perdidos.)
- um PC inicializável a partir de um dispositivo de mídia flash USB

△ **CUIDADO:** Alguns PCs mais antigos podem não ser inicializados a partir de um dispositivo de mídia flash USB. Se a ordem padrão de inicialização no Utilitário de Configuração (F10) do computador relaciona o dispositivo USB antes da unidade de disco rígido, é possível inicializar o computador de um dispositivo de mídia flash USB. Caso contrário, deve ser utilizado um disquete de inicialização.

1. Se houver alguma placa PCI no sistema ligada a unidades SCSI, ATA RAID ou SATA, desligue o computador e retire o cabo de alimentação.

△ **CUIDADO:** Você DEVE retirar o cabo de alimentação da tomada.

2. Abra o computador e remova as placas PCI.
3. Insira o dispositivo de mídia Flash USB em uma das portas USB do computador e remova todos os demais dispositivos de armazenamento USB, exceto as unidades de disquete USB. Feche a tampa do computador.
4. Conecte o cabo de alimentação na tomada e ligue o computador.
5. Assim que o computador estiver ligado, pressione **F10** antes que o computador inicialize o sistema operacional para entrar no utilitário de configuração. Pressione **Enter** para omitir a tela de abertura, se necessário.


 **NOTA:** Se a tecla **F10** não for pressionada no momento certo, você deverá reiniciar o computador e pressionar novamente **F10** antes que o computador inicialize o sistema operacional para acessar o utilitário.

6. Vá até **Advanced** (Dispositivos PCI) > **PCI Devices** (Avançados) para desativar tanto os controladores PATA quanto os SATA. Quando desativar o controlador SATA, anote a IRQ atribuída a ele. Você terá que reatribuir essa IRQ posteriormente. Saia da configuração e confirme as alterações.

IRQ SATA: _____

7. Insira um disquete DOS de inicialização com **FDISK.COM** e também **SYS.COM** ou **FORMAT.COM**, em uma unidade de disquete e ligue o computador para inicializar a partir do disquete DOS.
8. Execute **FDISK** e exclua todas as partições existentes no dispositivo de mídia Flash USB. Crie uma nova partição e marque-a como ativa. Saia de **FDISK** pressionando a tecla **Esc**.
9. Se o sistema não reinicializar automaticamente ao sair de **FDISK**, pressione as teclas **Ctrl+Alt+Del** para reinicializar pelo disquete DOS.
10. No prompt **A:** digite **FORMAT C: /S** e depois pressione **Enter**. **FORMAT** formatará o dispositivo de mídia Flash USB, acrescentará os arquivos de sistema e pedirá um Nome para a Unidade (Volume Label).
11. Pressione **Enter** para não nomear, ou digite um, se desejar.
12. Desligue o computador e retire o cabo de alimentação da tomada. Abra o computador e reinstale as placas PCI removidas anteriormente. Feche a tampa do computador.
13. Conecte o cabo de alimentação na tomada, remova o disquete e ligue o computador.
14. Assim que o computador estiver ligado, pressione **F10** antes que o computador inicialize o sistema operacional para entrar no utilitário de configuração. Pressione **Enter** para omitir a tela de abertura, se necessário.

15. Vá até **Advanced** (Dispositivos PCI) > **PCI Devices** (Avançados) e reative os controladores PATA e SATA desativados na etapa 6. Reatribua ao controlador SATA sua IRQ original.
16. Salve as alterações e saia. O computador inicializará pelo dispositivo de mídia flash USB como sendo a unidade C.

 **NOTA:** A sequência padrão de inicialização varia de um computador para outro e pode ser alterada no Utilitário de Configuração (F10) do Computador. Consulte o *Utilitário de Configuração (F10) do Computador* para obter instruções.

Se utilizou uma versão DOS do Windows 9x, poderá ser exibida rapidamente uma tela com o logotipo do Windows. Para não exibir essa tela, acrescente um arquivo de comprimento zero chamado LOGO.SYS ao diretório raiz do dispositivo de mídia flash USB.

Retorne para [Cópia para vários computadores na página 18](#).

8 Botão Liga/Desliga de Dois Estados

Com a interface de energia e configuração avançada (ACPI) ativada, o botão Liga/Desliga pode funcionar como interruptor Liga/Desliga ou como botão Modo de Espera. O recurso do modo Em espera não desliga completamente a alimentação mas, faz o computador entrar no modo de Espera para economia de energia. Isso permite que desligue rapidamente, sem fechar aplicativos, e retorne ao mesmo estado operacional sem perder dados.

Para alterar a configuração do botão Liga/Desliga, execute as seguintes etapas:

1. Clique com o botão esquerdo do mouse **Iniciar**, em seguida selecione **Painel de controle > Opções de energia**.
2. Em **Propriedades de opções de energia**, selecione a guia **Avançado**.
3. Na seção **Botão Liga/Desliga** selecione **Modo Em espera**.

Após configurar o botão Liga/Desliga para funcionar como botão modo Em espera, pressione o botão Liga/Desliga para colocar o sistema em um estado de mínimo consumo de energia (modo Em espera). Pressione novamente o botão para que o sistema volte rapidamente do modo Em espera para a plena potência. Para desligar completamente o sistema, mantenha o botão Liga/Desliga pressionado por quatro segundos.

△ **CUIDADO:** Não utilize o botão Liga/Desliga para desligar o computador a não ser que o sistema não responda, pois desligar a energia não sendo pelo sistema operacional pode provocar danos ou perdas de dados na unidade de disco rígido.

9 Web Site de Suporte HP

Os engenheiros da HP testam e depuram com rigor o software desenvolvido pela HP e por terceiros, e desenvolvem software específico para suporte ao sistema operacional, para garantir o desempenho, a compatibilidade e a confiabilidade dos computadores HP.

Ao fazer a transição para sistemas operacionais novos ou com novas versões, é importante implementar o software de suporte para tal sistema operacional. Para utilizar uma versão do Microsoft Windows diferente da que está no computador, instale os drivers de dispositivos e utilitários correspondentes para garantir que todos os recursos sejam admitidos e o funcionamento seja correto.

A HP tornou fácil a tarefa de localizar, acessar, avaliar e instalar o mais recente software de suporte. É possível fazer o download do software a partir de <http://www.hp.com.br/suporte>.

O Web site contém os mais recentes drivers de dispositivo, utilitários e imagens para flash da memória ROM necessários para utilizar o mais recente sistema operacional Microsoft Windows no computador HP.

10 Padrões da indústria


As soluções de gerenciamento da HP integram-se com outros aplicativos de gerenciamento de sistemas, com base em padrões da indústria, como:

- Web-Based Enterprise Management (WBEM)
- Windows Management Interface (WMI)
- Tecnologia Wake on LAN
- ACPI
- SMBIOS
- Suporte para execução antes da inicialização (PXE)

11 Rastreamento e segurança de equipamentos

Os recursos de rastreamento incorporados ao computador fornece dados chave de rastreamento de computadores, que podem ser gerenciados utilizando HP Systems Insight Manager, HP Client Manager, HP Configuration Management Solution, HP Client Configuration Manager, ou outros aplicativos de gerenciamento de sistemas. Uma integração completa e automática entre os recursos de rastreamento de computadores e esses produtos permite escolher a ferramenta de gerenciamento mais adequada ao ambiente e alavancar o investimento nas ferramentas existentes.

A HP também oferece várias soluções para controle de acesso a informações e componentes valiosos. O HP Embedded Security for ProtectTools, se instalado, evita o acesso não-autorizado a dados, verifica a integridade do sistema e autentica usuários externos que tentem acessar o sistema. (Para obter mais informações, consulte *HP ProtectTools Security Manager Guide* em <http://www.hp.com/products/security>.) Recursos de segurança como o HP Embedded Security for ProtectTools, o Sensor Inteligente de Tampa e o Bloqueio Inteligente de Tampa, disponíveis em determinados modelos, ajudam a evitar acesso não autorizado a componentes internos do computador pessoal. Ao desativar as portas paralela, serial ou USB, ou ao desativar o recurso de inicialização por mídia removível, você pode proteger dados valiosos. Os alertas de Alteração de Memória e o Sensor Inteligente de Tampa podem ser enviados automaticamente a aplicativos de gerenciamento do sistema para fornecer notificações pró-ativas de acesso não autorizado aos componentes internos do computador.

 **NOTA:** O HP Embedded Security for ProtectTools, o sensor inteligente de tampa e o bloqueio inteligente de tampa estão disponíveis como opções em alguns sistemas.

Utilize os seguintes utilitários para gerenciar as opções de segurança no computador HP:

- Localmente, utilizando o Utilitário Computer Setup. Consulte o *Guia do Utilitário Configuração (F10) do Computador* que acompanha o computador para obter mais informações e instruções sobre como usar os Utilitários Computer Setup.
- Remotamente, utilizando o HP Client Manager from Symantec, HP Client Automation ou System Software Manager. Estes softwares permitem a instalação segura, consistente e controle das configurações de segurança.

A tabela e as seções a seguir referem-se ao gerenciamento local dos recursos de segurança do computador, por intermédio do Utilitário de Configuração (F10) do computador.

Tabela 11-1 Visão Geral dos Recursos de Segurança

Opção	Descrição
Setup Password (Senha de configuração)	Permite definir e ativar a senha de configuração (administrador).

Tabela 11-1 Visão Geral dos Recursos de Segurança (continuação)

	<p>NOTA: Se houver uma senha de configuração definida, essa senha será necessária para alterar opções do Utilitário de Configuração, executar o flash da memória ROM e alterar determinadas configurações plug and play no Windows.</p>
<p>Power-On Password (Senha de Inicialização)</p>	<p>Permite que você defina e ative uma senha de inicialização. O prompt de senha de inicialização aparece após um ciclo de alimentação. Caso o usuário não digite a senha de inicialização correta, a unidade não iniciará.</p> <p>NOTA: Esta senha não aparece em inicializações a quente, assim como Ctrl+Alt+Delete ou Reiniciar a partir do Windows, a não ser que esteja selecionada em Password Options (Opções de Senhas) (vide abaixo).</p>
<p>Password Options (Opções de Senha)</p> <p>(Essa seleção aparece somente se houve o estabelecimento de uma senha de inicialização ou de configuração.)</p>	<p>Permite:</p> <ul style="list-style-type: none">• Bloquear recursos legados (aparece somente se uma senha de configuração for estabelecida)• Ativar/desativar modo de servidor de rede (aparece somente se uma senha de inicialização for estabelecida)• Permite especificar se a senha é necessária para inicialização a quente (Ctrl+Alt+Delete) (aparece se houver uma senha de inicialização definida)• Ativar/desativar configurar modo procurar (aparece se uma senha for definida) (permite visualizar, porém não alterar, as opções do Utilitário de Configuração (F10) sem inserir uma senha de configuração)• Ativar/desativar Stringent Password (Senha Rigorosa) (aparece se uma senha de ativação estiver definida), quando qualquer ativada ignora no jumper de senha integrada para desativar a senha de inicialização. <p>Consulte o <i>Guia de Gerenciamento de Desktop</i> para obter mais informações.</p>
<p>Smart Cover (Tampa Inteligente) (alguns modelos)</p>	<p>Permite que:</p> <ul style="list-style-type: none">• Trave/destrave o bloqueio da tampa.• Configure o sensor de remoção da tampa para desativar/notificar usuário/configurar senha. <p>NOTA: <i>Notificar usuário:</i> alerta o usuário de que o sensor detectou que a tampa foi removida. <i>Senha de configuração:</i> exige que a senha de configuração seja inserida para inicializar o computador, se o sensor detectar que a tampa foi removida.</p> <p>Esse recurso é admitido apenas em alguns modelos.</p>
<p>Device Security (Segurança do Dispositivo)</p>	<p>Permite que você defina Dispositivo Disponível/Dispositivo Oculto para:</p> <ul style="list-style-type: none">• Portas seriais• Porta paralela• Portas USB traseiras• Portas USB frontais• Portas USB internas• Áudio do sistema• Controladores de rede (determinados modelos)• Disquete legado• Dispositivo de embedded security (determinados modelos)• SATA0• SATA1 (alguns modelos)

Tabela 11-1 Visão Geral dos Recursos de Segurança (continuação)

	<ul style="list-style-type: none">• SATA2 (alguns modelos)• SATA3 (alguns modelos)• eSATA (alguns modelos)
LoJack for HP ProtectTools	<p>Permite a você monitorar, gerenciar e rastrear remotamente seu computador.</p> <p>Uma vez ativado, o LoJack Pro for HP ProtectTools é configurado a partir do Absolute Software Customer Center. A partir do Centro do Cliente, o administrador pode configurar o LoJack for HP ProtectTools para monitorar ou gerenciar o computador. Se o sistema é colocado em lugar errado ou roubado, o Centro do Cliente pode dar assistência às autoridades locais para localizar e recuperar o computador. Se configurado, o LoJack Pro pode continuar a funcionar mesmo se a unidade de disco rígido for apagada ou substituída.</p>
Network Service Boot (Inicialização por Serviço de Rede)	Ativa/desativa a capacidade do computador de ser inicializado a partir de um sistema operacional instalado em um servidor de rede. (Esse recurso está disponível apenas em modelos com NIC; o controlador de rede precisa ser uma placa de expansão PCI ou estar integrado na placa do sistema.)
System IDs (IDs do Sistema)	<p>Permite definir:</p> <ul style="list-style-type: none">• Etiqueta de equipamento (identificador de 18 bytes), um número de identificação de propriedade atribuído pela companhia para o computador.• Etiqueta de propriedade (identificador de 80 bytes) exibido durante o POST.• Número de série do chassi ou número do identificador exclusivo universal (UUID). O UUID só pode ser atualizado se o número de série atual do chassi for inválido. (Esses números de ID são normalmente definidos na fábrica e são utilizados para identificar o sistema de maneira exclusiva.)• A configuração local do teclado (por exemplo, inglês ou alemão) para a entrada do ID do sistema.
DriveLock Security (Segurança DriveLock)	<p>Permite atribuir ou modificar uma senha mestre ou de usuário para unidades de disco rígido. Quando esse recurso estiver ativado, o usuário será solicitado a fornecer uma das senhas do DriveLock durante o POST. Se nenhuma delas for inserida corretamente, a unidade de disco rígido permanecerá inacessível até que uma das senhas seja inserida corretamente durante a inicialização a frio subsequente.</p> <p>NOTA: Essa seleção será exibida somente quando pelo menos uma unidade MultiBay que admita o recurso DriveLock estiver conectada ao sistema.</p>
Setup Security Level (Nível de Segurança de Configuração)	<p>Oferece um método que oferece a usuários finais o acesso limitado à alteração de opções de configuração especificadas, sem ter que conhecer a senha de configuração.</p> <p>Este recurso proporciona aos administradores a flexibilidade para proteger alterações em opções de configuração essenciais, enquanto permitem que o usuário visualize as configurações do sistema e defina as opções que não são essenciais. O administrador especifica os direitos de acesso nas opções de configuração individuais caso a caso, via menu nível de segurança de configuração. Por padrão, todas as opções de configuração recebem uma senha de configuração, indicando que o usuário deve digitar a senha de configuração correta durante o POST para fazer as alterações nas opções. O administrador pode definir itens individuais para ninguém, indicando que os usuários podem fazer alterações em opções específicas, quando a configuração é acessada com senhas incorretas. A opção nenhuma é substituída por senha de inicialização se houver uma ativada.</p> <p>NOTA: Configurar modo de busca deve estar ativado para que o usuário possa acessar a configuração sem precisar digitar a senha.</p>
System Security (Segurança do Sistema) (alguns modelos: essas opções são dependentes do hardware)	<p>O modo de Prevenção contra Execução de Dados (alguns modelos) (ativado/desativado) - Ajuda a prevenir violações de segurança no sistema operacional.</p> <p>Tecnologia de Virtualização (Virtualization Technology) (alguns modelos) (ativado/desativado) - Controla os recursos de virtualização do processador. Alterar essa configuração exige que desligue e ligue novamente o computador.</p>

Tabela 11-1 Visão Geral dos Recursos de Segurança (continuação)

E/S Direcionada para Tecnologia de Virtualização (alguns modelos) (ativado/desativado) - Controla os recursos de remapeamento DMA de virtualização do chipset. Alterar essa configuração exige que desligue e ligue novamente o computador.

Tecnologia de Execução Confiável (Trusted Execution Technology) (alguns modelos) (ativado/desativado) - Controla os recursos de chipset e processador subjacente necessários para admitir dispositivo virtual. Alterar essa configuração exige que desligue e ligue novamente o computador. Para ativar esse recurso você deve ativar os seguintes recursos:

- Suporte do Dispositivo de Embedded Security
- Tecnologia de Virtualização
- E/S Direcionada a Tecnologia de Virtualização

Suporte de Dispositivo Embedded Security (alguns modelos) (ativado/desativado) - Permite a ativação e desativação do Dispositivo Embedded Security. Alterar essa configuração exige que desligue e ligue novamente o computador.

NOTA: Para configurar o Dispositivo Embedded Security, uma senha de Configuração deve ser definida.

- Restaurar para Definições de Fábrica (alguns modelos) (Não restaurar/Restaurar) - Restaurar para os padrões de fábrica apagará todas as chaves de segurança. Alterar essa configuração exige que desligue e ligue novamente o computador.

CUIDADO: O dispositivo embedded security é um componente decisivo de vários esquemas de segurança. Apagar as chaves de segurança impede o acesso a dados protegidos pelo Dispositivo Embedded Security. Escolher Restaurar para as Definições de Fábrica pode resultar em significativa perda de dados.

- Restaurar credenciais de autenticação (alguns modelos) (Não restaurar/Restaurar) - Selecionando Restaurar desativa o suporte de autenticação de inicialização e limpa a informação de autenticação a partir do Dispositivo Embedded Security. Alterar essa configuração exige que desligue e ligue novamente o computador.

Gerenciamento do sistema operacional do Dispositivo Embedded Security (alguns modelos) - Esta opção permite ao usuário limitar o controle do sistema operacional do Dispositivo Embedded Security. Alterar essa configuração exige que desligue e ligue novamente o computador. Esta opção permite ao usuário limitar o controle do sistema operacional do Dispositivo Embedded Security.

- Restaurar a partir do Dispositivo Embedded Security (alguns modelos) (ativado/desativado) - Esta opção permite ao usuário limitar a capacidade do sistema operacional para solicitar uma Restauração para as Definições de Fábrica a partir do Dispositivo Embedded Security. Alterar essa configuração exige que desligue e ligue novamente o computador.


NOTA: Para ativas esta opção, uma senha de Configuração deve ser definida.

PAVP (Alguns modelos) (desativado/mínimo/máximo) - PAVP ativa o Path de Vídeo e Áudio Protegido no Chipset. Este caminho permite a visualização de alguns conteúdos de alta definição protegidos que quanto ao mais seria proibida a reprodução. Selecionando Máximo, irá atribuir 96 Megabytes de memória do sistema exclusivamente para PAVP.

Segurança de Senha

A senha de inicialização evita o uso não autorizado do computador ao exigir a digitação de senha para ter acesso a aplicativos ou a dados, cada vez que o computador é ligado ou reinicializado. A senha de configuração evita especificamente o acesso não autorizado no Utilitário de Configuração pode servir para ignorar a senha de inicialização. Em outras palavras, quando a senha de inicialização for solicitada, a digitação da senha de configuração em seu lugar permitirá acesso ao computador.

É possível definir uma senha para toda a rede para que o administrador do sistema possa conectar-se a todos os sistemas da rede para efetuar manutenção sem a necessidade de saber a senha de inicialização, mesmo que tal senha tenha sido definida.


 **NOTA:** O System Software Manager (SSM) pode ser usado para criar e gerenciar senhas do BIOS com o sistema operacional Windows. Para obter mais informações consulte o Guia do Usuário do SSM em <http://www.hp.com/go/ssm>.

NOTA: A HP Client Management Interface (HP CMI) fornece acesso ao gerenciamento de configuração do BIOS incluindo senhas do BIOS em sistema operacional Windows. Para obter mais informação consulte a Documentação Técnica do HP Client Management Interface em <http://www.hp.com/go/hpcmi>.

Definição de uma senha de configuração através do Utilitário de Configuração

Se o sistema estiver equipado com um dispositivo embedded security, consulte o Guia *HP ProtectTools Security Manager* em <http://www.hp.com.br>. Estabelecer uma senha de configuração através do Utilitário de Configuração impede a reconfiguração do computador (use o Utilitário de Configuração (F10) do Computador) até que a senha seja digitada.

1. Ligue ou reinicie o computador. Se estiver no Windows, clique em **Iniciar > Desligar > Reiniciar**.
2. Assim que o computador estiver ligado, pressione **F10** antes que o computador inicialize o sistema operacional para entrar no utilitário de configuração. Pressione **Enter** para omitir a tela de abertura, se necessário.

 **NOTA:** Se a tecla **F10** não for pressionada no momento certo, você deverá reiniciar o computador e pressionar novamente **F10** antes que o computador inicialize o sistema operacional para acessar o utilitário.


3. Selecione **Security** (Segurança), em seguida selecione **Setup Password** (Senha de Configuração) e siga as instruções na tela.
4. Antes de sair, clique em **File** (Arquivo) > **Save Changes and Exit** (Salvar alterações e sair).

Estabelecendo uma senha de inicialização utilizando o Utilitário de Configuração

Definir uma senha de inicialização por intermédio do Utilitário de Configuração evita o acesso ao computador ao ligá-lo, a não ser que seja digitada a senha. Quando a senha de inicialização é definida, o Utilitário de Configuração apresenta **Password Options** (Opções de Senha) no menu **Security** (Segurança). As opções de senha incluem **Password Prompt on Warm Boot** (Solicitar senha em

inicialização a quente). Quando **Password Prompt on Warm Boot** (Solicitar senha em inicialização a quente) ativado, é necessário digitar a senha a cada inicialização do computador.

1. Ligue ou reinicie o computador. Se estiver no Windows, clique em **Iniciar > Desligar > Reiniciar**.
2. Assim que o computador estiver ligado, pressione **F10** antes que o computador inicialize o sistema operacional para entrar no utilitário de configuração. Pressione **Enter** para omitir a tela de abertura, se necessário.


 **NOTA:** Se a tecla **F10** não for pressionada no momento certo, você deverá reiniciar o computador e pressionar novamente **F10** antes que o computador inicialize o sistema operacional para acessar o utilitário.

3. Selecione **Security** (Segurança), em seguida selecione **Power-On Password** (Senha de Configuração) e siga as instruções na tela.
4. Antes de sair, clique em **File** (Arquivo) > **Save Changes and Exit** (Salvar alterações e sair).

Inserção de uma senha de inicialização

Para digitar uma senha de inicialização, siga as seguintes etapas:

1. Ligue ou reinicie o computador. Se estiver no Windows, clique em **Iniciar > Desligar > Reiniciar o computador**.
2. Quando é exibido o ícone da chave no monitor, digite a senha atual e pressione **Enter**.

 **NOTA:** Digite cuidadosamente; por segurança, os caracteres digitados não são exibidos na tela.


Se digitar a senha errada, é exibido um ícone de uma chave quebrada. Tente novamente. Após três tentativas malsucedidas, você terá de desligar o computador e religá-lo, antes de tentar novamente.

Digitação da senha de configuração


Se o sistema estiver equipado com um dispositivo embedded security, consulte o Guia *HP ProtectTools Security Manager* em <http://www.hp.com.br>.

Se foi definida uma senha de configuração no computador, você será solicitado a digitá-la toda vez que executar o utilitário de de configuração.

1. Ligue ou reinicie o computador. Se estiver no Windows, clique em **Iniciar > Desligar > Reiniciar**.
2. Assim que o computador estiver ligado, pressione **F10** antes que o computador inicialize o sistema operacional para entrar no utilitário de configuração. Pressione **Enter** para omitir a tela de abertura, se necessário.

 **NOTA:** Se a tecla **F10** não for pressionada no momento certo, você deverá reiniciar o computador e pressionar novamente **F10** antes que o computador inicialize o sistema operacional para acessar o utilitário.

3. Quando for exibido o ícone da chave no monitor, digite a senha atual e pressione **Enter**.

 **NOTA:** Digite cuidadosamente; por segurança, os caracteres digitados não são exibidos na tela.


Se digitar a senha errada, é exibido um ícone de uma chave quebrada. Tente novamente. Após três tentativas malsucedidas, você terá de desligar o computador e religá-lo, antes de tentar novamente.

Alteração de uma senha de inicialização ou configuração


Se o sistema estiver equipado com um dispositivo embedded security, consulte o Guia *HP ProtectTools Security Manager* em <http://www.hp.com.br>.

1. Ligue ou reinicie o computador. Se estiver no Windows, clique em **Iniciar > Desligar > Reiniciar o computador**.
2. Para alterar a senha de inicialização, vá para o passo 3.

Para alterar a senha de Configuração, assim que o computador estiver ligado, pressione **F10** antes que o computador inicialize o sistema operacional para entrar no Utilitário de Configuração. Pressione **Enter** para omitir a tela de abertura, se necessário.


 **NOTA:** Se a tecla **F10** não for pressionada no momento certo, você deverá reiniciar o computador e pressionar novamente **F10** antes que o computador inicialize o sistema operacional para acessar o utilitário.

3. Quando for exibido o ícone da chave, digite a senha atual, uma barra (/) ou outro caractere delimitador, a nova senha, outra barra (/) ou outro caractere delimitador, e novamente a nova senha, conforme mostrado: `senha atual/nova senha/nova senha`

 **NOTA:** Digite cuidadosamente; por segurança, os caracteres digitados não são exibidos na tela.

4. Pressione **Enter**.

A nova senha é válida na próxima vez em que o computador for ligado.


 **NOTA:** Consulte [Caracteres delimitadores no teclado nacional na página 33](#) para obter informações sobre outros caracteres delimitadores. A senha de inicialização e/ou a senha de configuração também pode ser alterada utilizando as opções de Segurança no Utilitário de Configuração.

Exclusão de uma senha de inicialização ou configuração


Se o sistema estiver equipado com um dispositivo embedded security, consulte o Guia *HP ProtectTools Security Manager* em <http://www.hp.com.br>.

1. Ligue ou reinicie o computador. Se estiver no Windows, clique em **Iniciar > Desligar > Reiniciar o computador**.
2. Para excluir a senha de inicialização, vá para a etapa 3.

Para excluir a senha de Configuração, assim que o computador estiver ligado, pressione **F10** antes que o computador inicialize o sistema operacional para entrar no utilitário de configuração. Pressione **Enter** para omitir a tela de abertura, se necessário.

 **NOTA:** Se a tecla **F10** não for pressionada no momento certo, você deverá reiniciar o computador e pressionar novamente **F10** antes que o computador inicialize o sistema operacional para acessar o utilitário.

3. Quando for exibido o ícone da chave, digite a senha atual seguida por uma barra (/) ou outro caractere delimitador, conforme mostrado: `senha atual/`
4. Pressione **Enter**.

 **NOTA:** Consulte [Caracteres delimitadores no teclado nacional na página 33](#) para obter informações sobre outros caracteres delimitadores. A senha de inicialização e/ou a senha de configuração também pode ser alterada utilizando as opções de Segurança no Utilitário de Configuração.

Caracteres delimitadores no teclado nacional

Cada teclado é projetado para atender a requisitos específicos de um país. A sintaxe e as teclas utilizadas para alterar ou excluir a senha dependem do teclado fornecido com o computador.

Caracteres Delimitadores no Teclado Nacional			
/	Árabe	- Grego	/ Russo
=	Belga	. Hebraico	- Eslovaco
-	BHCMSE*	- Húngaro	- Espanhol
/	Português brasileiro	- Italiano	/ Sueco/Finlandês
/	Chinês	/ Japonês	- Suíço
-	Tcheco	/ Coreano	/ Taiwan
-	Dinamarquês	- América Latina	/ Tailandês
!	Francês	- Norueguês	. Turco
é	Francês Canadense	- Polonês	/ Inglês americano
-	Alemão	- Português	

* Para Bósnia-Herzegovina, Croácia, Montenegro, Sérvia e Eslovênia

Limpeza de senhas

Se você esquecer a senha, não será possível acessar o computador. Consulte o *Guia de Solução de Problemas* para obter instruções sobre como cancelar senhas.

Se o sistema estiver equipado com um dispositivo embedded security, consulte o Guia *HP ProtectTools Security Manager* em <http://www.hp.com.br>.

DriveLock

DriveLock é um recurso padrão da indústria que evita o acesso não autorizado a dados em unidades de discos rígidos ATA. O DriveLock foi implementado como uma extensão do Utilitário de Configuração. Ele está disponível somente quando unidades de disco rígido, que admitem o conjunto de comandos de segurança ATA, são detectados. O DriveLock destina-se aos clientes da HP para os quais a segurança dos dados é a principal preocupação. Para esses clientes, o custo da unidade de disco rígido e a perda dos dados nela armazenados não têm tanta importância comparados aos danos que poderiam resultar do acesso não autorizado ao seu conteúdo. Para equilibrar este nível de segurança e a necessidade de contornar na prática o esquecimento de uma senha, a implementação do DriveLock pela HP emprega um esquema de segurança de duas senhas. Uma senha é para ser definida e utilizada por um administrador de sistema, enquanto a outra normalmente é definida e utilizada pelo usuário final. Não existe uma "porta dos fundos" que possa servir para destravar a unidade se as duas senhas forem esquecidas. Entretanto, o DriveLock oferece maior segurança quando os dados armazenados no disco rígido são copiados em um sistema de informações corporativo ou quando são feitos backups

dos dados regularmente. Na eventualidade de ambas as senhas do DriveLock serem perdidas, a unidade de disco rígido não poderá ser utilizada. Para os usuários que não se enquadram no perfil de cliente definido previamente, esse pode ser um risco inaceitável. Para os usuários que se enquadram nesse perfil de cliente, esse risco pode ser tolerado tendo em vista a natureza dos dados armazenados na unidade de disco rígido.

Utilização do DriveLock

Quando uma ou mais unidades que oferecem suporte ao comando de segurança ATA são detectadas, a opção DriveLock é exibida abaixo do menu Security no Utilitário de Configuração. O usuário conta com opções para definir a senha principal ou ativar o DriveLock. A senha de usuário deve ser fornecida para ativar o DriveLock. Tendo em vista que a configuração inicial do DriveLock em geral é efetuada por um administrador de sistema, a senha principal deve ser definida primeiramente. A HP aconselha os administradores de sistema a definir a senha principal, quer eles planejem ativar o DriveLock quer planejem mantê-lo desativado. A senha principal permitirá que o administrador modifique as definições do DriveLock se a unidade porventura ficar travada. Depois que a senha principal for definida, o administrador do sistema pode ativar o DriveLock ou optar por mantê-lo desativado.

Se houver uma unidade de disco rígido bloqueada, o POST exigirá uma senha para desbloquear o dispositivo. Se uma senha de ativação tiver sido definida e coincidir com a senha de usuário do dispositivo, o POST não solicitará ao usuário que insira novamente a senha. De outra forma, o usuário será solicitado a inserir uma senha do DriveLock. Na inicialização a frio, deverá ser utilizada a senha principal ou a senha de usuário. Na inicialização a quente, digite a mesma senha utilizada para desbloquear a unidade durante o procedimento de inicialização a frio. Os usuários terão duas possibilidades para inserir a senha correta. Na inicialização a frio, se nenhuma tentativa for bem-sucedida, o POST continuará, mas a unidade permanecerá inacessível. Na inicialização a quente ou na reinicialização do Windows, se ambas as tentativas fracassarem, o POST suspenderá e o usuário será instruído a distribuir a energia.

Aplicativos do DriveLock

A utilização mais prática do recurso de segurança DriveLock ocorre em um ambiente corporativo. O administrador de sistema é responsável por configurar a unidade de disco rígido MultiBay, o que envolve, dentre outras coisas, definir a senha principal do DriveLock e uma senha de usuário temporária. Na eventualidade de o usuário esquecer a senha de usuário ou de o equipamento ser transferido a outro funcionário, a senha principal poderá sempre ser utilizada para restaurar a senha de usuário e recuperar o acesso à unidade de disco rígido.

A HP recomenda que os administradores do sistema corporativo que optem por ativar o DriveLock também estabeleçam uma política corporativa para definir e manter senhas mestre. Isso poderia ser feito para evitar a situação em que um funcionário, intencionalmente ou não, defina ambas as senhas do DriveLock antes de demitir-se da empresa. Nesse caso, a unidade de disco rígido ficaria inutilizável e precisaria ser substituída. Da mesma forma, se os administradores de sistema não definirem a senha principal, poderão deparar com uma situação em que não terão acesso à unidade de disco rígido e não poderão executar verificações de rotina de software não autorizado, outras funções de controle de equipamento e suporte.

Para usuários com exigências de segurança menos rigorosas, a HP não recomenda a ativação do DriveLock. Os usuários que se enquadram nessa categoria incluem pessoas físicas e usuários que normalmente não mantêm dados secretos nas unidades de disco rígido. Para esses usuários, a possibilidade de perda de uma unidade de disco rígido em decorrência de esquecimento de ambas as senhas é mais onerosa que o valor dos dados aos quais o DriveLock foi designado a proteger. O acesso ao Utilitário de Configuração e ao DriveLock pode ser restringido por meio da senha de configuração. Ao especificar uma senha de configuração e não fornecê-la aos usuários finais, os administradores do sistema podem impedir que os usuários ativem o DriveLock.

Sensor inteligente de tampa

O Sensor de Remoção da Tampa, disponível em alguns modelos, é uma combinação de tecnologia de hardware e software que pode alertar quando a tampa ou o painel lateral do computador forem removidos. Existem três níveis de proteção, descritos na tabela a seguir.


Tabela 11-2 Níveis de proteção do sensor inteligente de tampa

Nível	Configuração	Descrição
Nível 0	Desativado	O sensor inteligente de tampa está desativado (padrão).
Nível 1	Notificar usuário	Ao reinicializar o computador, é exibida uma mensagem na tela indicando que a tampa ou o painel lateral do computador foi removida (o).
Nível 2	Senha de configuração	Ao reinicializar o computador, é exibida uma mensagem na tela indicando que a tampa ou o painel lateral do computador foi removida (o). Deve digitar a senha de configuração para prosseguir.

NOTA: Essas definições podem ser alteradas usando Configuração do Computador. Para obter mais informações sobre Configuração do Computador, consulte o Guia do *Utilitário de Configuração (F10) do computador*.


Definição do nível de proteção do sensor inteligente de tampa

Para definir o nível de proteção do sensor inteligente de tampa, siga estas etapas:

1. Ligue ou reinicie o computador. Se estiver no Windows, clique em **Iniciar > Desligar > Reiniciar**.
2. Assim que o computador estiver ligado, pressione **F10** antes que o computador inicialize o sistema operacional para entrar no utilitário de configuração. Pressione **Enter** para omitir a tela de abertura, se necessário.
 **NOTA:** Se a tecla **F10** não for pressionada no momento certo, você deverá reiniciar o computador e pressionar novamente **F10** antes que o computador inicialize o sistema operacional para acessar o utilitário.
3. Selecione **Security** (Segurança) > **Smart Cover** (Tampa Inteligente) > **Cover Removal Sensor** (Sensor de Remoção da Tampa), e selecione o nível de segurança desejado.
4. Antes de sair, clique em **File** (Arquivo) > **Save Changes and Exit** (Salvar alterações e sair).

Bloqueio Inteligente de Tampa

O Bloqueio inteligente de tampa é uma trava de tampa controlável por software disponível em alguns computadores HP. Essa trava evita o acesso não-autorizado aos componentes internos do computador. O computador é fornecido com o bloqueio inteligente de tampa na posição desbloqueado.


 **CUIDADO:** Para máxima segurança do bloqueio da tampa, defina uma senha de configuração. A senha de configuração evita o acesso não autorizado no utilitário de configuração.

 **NOTA:** O bloqueio inteligente de tampa está disponível como opcional em determinados sistemas.

Ativação do bloqueio inteligente de tampa

Para ativar e travar o bloqueio inteligente de tampa, siga estas etapas:


1. Ligue ou reinicie o computador. Se estiver no Windows, clique em **Iniciar > Desligar > Reiniciar**.
2. Assim que o computador estiver ligado, pressione **F10** antes que o computador inicialize o sistema operacional para entrar no utilitário de configuração. Pressione **Enter** para omitir a tela de abertura, se necessário.

 **NOTA:** Se a tecla **F10** não for pressionada no momento certo, você deverá reiniciar o computador e pressionar novamente **F10** antes que o computador inicialize o sistema operacional para acessar o utilitário.

3. Selecione **Security** (Segurança) > **Smart Cover** (Tampa Inteligente) > **Cover Lock** (Bloqueio de Tampa) > **Lock option** (opção Bloqueio).
4. Antes de sair, clique em **File** (Arquivo) > **Save Changes and Exit** (Salvar alterações e sair).

Desativação do bloqueio inteligente de tampa

1. Ligue ou reinicie o computador. Se estiver no Windows, clique em **Iniciar > Desligar > Reiniciar**.
2. Assim que o computador estiver ligado, pressione **F10** antes que o computador inicialize o sistema operacional para entrar no utilitário de configuração. Pressione **Enter** para omitir a tela de abertura, se necessário.

 **NOTA:** Se a tecla **F10** não for pressionada no momento certo, você deverá reiniciar o computador e pressionar novamente **F10** antes que o computador inicialize o sistema operacional para acessar o utilitário.

3. Selecione **Security** (Segurança) > **Smart Cover** (Tampa Inteligente) > **Cover Lock** (Bloqueio de Tampa) > **Unlock** (Desbloquear).
4. Antes de sair, clique em **File** (Arquivo) > **Save Change** (Salvar alterações e sair).

Utilização da Chave à Prova de Falhas do Bloqueio Inteligente da Tampa

Se ativar o sensor inteligente de tampa e não puder digitar a senha para desativar o bloqueio, será necessário utilizar uma chave de segurança à prova de falhas para bloqueio inteligente de tampa para abrir a tampa do computador. Precisarás dessa chave em qualquer uma das seguintes circunstâncias:

- Falta de energia
- Falha na inicialização
- Falha em algum componente do PC (como o processador ou a fonte de alimentação)
- Esquecimento da senha

△ **CUIDADO:** A Chave à Prova de Falhas da Tampa Inteligente é uma ferramenta especializada que pode ser obtida na HP. Seja cauteloso, e solicite essa chave a um revendedor ou uma assistência técnica autorizada HP antes de precisar dela.

Para obter a chave de segurança à prova de falhas, utilize um dos métodos a seguir:

- Entre em contato com um revendedor ou uma assistência técnica autorizada da HP
- Ligue para o número apropriado listado na garantia

Para obter mais informações sobre o uso da Chave FailSafe da Smart Cover, consulte o *Guia de Referência de Hardware*.


Provisão de bloqueio de cabo

O painel traseiro do computador (alguns modelos) tem um bloqueio de cabo que permite prender fisicamente o computador a uma área de trabalho.

Para obter orientação com ilustrações, consulte o *Guia de Referência de Hardware*.

Tecnologia de identificação de impressão digital

Ao eliminar a necessidade de digitar senhas de usuário, a tecnologia de identificação de impressão digital HP aprimora a segurança da rede, simplifica o processo de conexão e reduz os custos associados ao gerenciamento de redes corporativas. Com preço acessível, não é restrito apenas a organizações de alta tecnologia e alta segurança.

 **NOTA:** O Suporte para tecnologia de identificação de impressão digital varia de acordo com o modelo.

Notificação e Recuperação de Falhas

Os recursos de notificação e recuperação de falhas combinam tecnologias inovadoras de hardware e software para evitar a perda de dados críticos e minimizar interrupções não planejadas.

Se o computador estiver conectado a uma rede gerenciada pelo HP Client Manager, o computador envia uma notificação de falha ao aplicativo de gerenciamento de rede. Com o Software HP Client Manager, é possível programar diagnósticos remotamente para executar automaticamente em todos os PCs e criar um relatório detalhado dos testes com falhas.

Sistema de proteção de unidade

O Sistema de proteção de unidade (DPS) é uma ferramenta de diagnóstico interna integrada nas unidades de disco rígido de alguns computadores HP. O DPS foi projetado para ajudar a diagnosticar problemas que possam resultar na substituição injustificada da unidade de disco rígido.

Quando os computadores HP são construídos, cada unidade de disco rígido instalada é testada por meio do DPS e um registro permanente de informações importantes é gravado na unidade. Toda vez que o DPS é executado, os resultados do teste são gravados na unidade de disco rígido. A assistência técnica autorizada pode utilizar essas informações para ajudar a diagnosticar as condições que levaram você a executar o software DPS. Consulte o *Guia de Solução de Problemas* para obter instruções sobre como usar o DPS.

Fonte de alimentação tolerante a picos de energia

Uma fonte de alimentação integrada tolerante a picos de energia oferece maior confiabilidade quando o computador é atingido por um pico de energia imprevisto na alimentação elétrica. A fonte de

alimentação é projetada para resistir a um pico de energia de potência de até 2.000 volts sem interrupção da operação do sistema nem perda de dados.

Sensor térmico

O sensor térmico é um recurso de hardware e software que monitora a temperatura interna do computador. Esse recurso exibe uma mensagem de cuidado quando a faixa normal é ultrapassada, o que permite agir antes que componentes internos sejam danificados ou haja perda de dados.

△ **CUIDADO:** Uma condição de alta temperatura pode resultar em danos para o sistema ou perda de dados.

Índice

A

acesso ao computador,
controle 26
alteração de senha 32
Altiris
Client Management Suite 9
ativação do Bloqueio inteligente de
tampa 36

B

BIOS
Flash Remoto da Memória
ROM 14
HPQFlash 14
modo de recuperação de
emergência do bloco de
inicialização 15
bloqueio da tampa 35
Bloqueio da Tampa Inteligente
Chave à Prova de Falhas 36
bloqueio inteligente de tampa
ativação 36
desativação 36
Bloqueio Inteligente de
Tampa 35
Boot Block Emergency Recovery
Mode (Modo de recuperação de
emergência do bloco de
inicialização) 15
botão Liga/Desliga de dois
estados 23

C

caracteres delimitadores,
tabela 33
caracteres Delimitadores no
teclado, nacional 33
caracteres delimitadores no teclado
nacional 33

Chave à Prova de Falhas,
solicitação 36
Chave à Prova de Falhas da Tampa
Inteligente, solicitação 36
Client Management Interface 5
Client Manager from Symantec 8
configuração
cópia de múltiplos
computadores 18
cópia para um computador 17
inicial 2
configuração de instalação ,
replicação 17
configuração do botão liga/
desliga 23
configuração do botão Liga/
Desliga 23
configuração inicial 2
configuração remota 4
controle de acesso ao
computador 26
controle de equipamentos 26

D

desativação do Bloqueio inteligente
de tampa 36
dispositivo de inicialização
criação 19
dispositivo de mídia flash
USB 19
dispositivo de mídia flash USB,
inicializável 19, 20
DriveLock 33

E

Emergency Recovery Mode, Boot
Block 15
Endereço na Internet. *Consulte*
Web sites
exclusão de senha 32

F

ferramenta de diagnósticos para
unidades de disco rígido 37
ferramentas de clonagem,
software 2
ferramentas de implantação,
software 2
Flash de memória ROM 14
Flash Remoto da Memória
ROM 14
fonte de alimentação, tolerante a
picos de energia 37
fonte de alimentação tolerante a
picos de energia 37

H

HP
Catálogo de Clientes de
Produtos SMS para o Centro
de Sistema Microsoft 10
Client Management
Interface 5
Client Manager from
Symantec 8
Edições HP Client Automation
Starter, Standard e
Enterprise 8
ProtectTools Security
Manager 7
System Software Manager 6
HP Client Automation Enterprise
Edition 8
HP Client Manager 3
HPQFlash 14

I

imagem do software pré-
instalado 2

- inserção
 - senha de configuração 31
 - senha de inicialização 31
- L**
- limpeza de senhas 33
- M**
- mudança de sistema operacional, suporte 24
- N**
- notificação de alteração 13
- Notificação e Recuperação de Falhas 37
- Notificação Pró-Ativa de Alteração (PCN) 13
- P**
- padrões da indústria 25
- proteção da unidade de disco rígido 37
- ProtectTools Security Manager 7
- provisão de bloqueio de cabo 37
- PXE (Ambiente de execução pré-Inicialização) 4
- PXE – Ambiente de execução pré-inicialização 4
- R**
- Recovery Mode, Boot Block Emergency 15
- recuperação, software 2
- Remote System Installation 4
- S**
- segurança
 - Bloqueio Inteligente de Tampa 35
 - configurações 26
 - DriveLock 33
 - ProtectTools Security Manager 7
 - recursos; tabela 26
 - senha 29
 - sensor inteligente de tampa 35
 - tecnologia de identificação de impressão digital 37
 - trava de cabo 37
- senha
 - alteração 32
 - configuração 30, 31
 - de inicialização 30, 31
 - excluir 32
 - limpeza 33
 - segurança 29
- senha de configuração
 - alteração 32
 - configuração 30
 - excluir 32
 - inserção 31
- senha de inicialização
 - alteração 32
 - configuração 30
 - excluir 32
 - inserção 31
- sensor inteligente de tampa
 - configuração 35
 - níveis de proteção 35
- sensor térmico 38
- software
 - Altiris Client Management Suite 9
 - Catálogo de Clientes HP de Produtos SMS para o Centro de Sistema Microsoft 10
 - controle de equipamentos 26
 - Edições HP Client Automation Starter, Standard e Enterprise 8
 - ferramentas de atualizações e gerenciamento 5
 - gerenciador de segurança HP ProtectTools 7
 - HP Client Management Interface 5
 - HP Client Manager from Symantec 8
 - HP System Software Manager 6
 - implantação 2
 - integração 2
 - Notificação Pró-Ativa de Alteração (PCN) 13
 - recuperação 2
 - Remote System Installation 4
 - sistema de proteção de unidade 37
- Tecnologia de Gerenciamento Remoto 10
- Verdiem Surveyor 13
- solicitação de uma Chave à Prova de Falhas 36
- soluções descontinuadas 13
- Subscriber's Choice 13
- System Software Manager 6
- T**
- Tecnologia de Gerenciamento Remoto 10
- tecnologia de identificação de impressão digital 37
- temperatura, interna do computador 38
- temperatura interna do computador 38
- U**
- unidade, proteção 37
- unidades de disco rígido, ferramenta de diagnósticos 37
- V**
- Verdiem Surveyor 13
- W**
- Web sites
 - Altiris Client Management Suite 10
 - Catálogo de Clientes HP para Microsoft SMS 10
 - Download do BIOS 14
 - Downloads de Driver e Software 18
 - Flash de memória ROM 14
 - Flash Remoto da Memória ROM 14
 - HP Client Automation Agent 3
 - HP Client Automation Center 8
 - HP Client Manager 3
 - HP Client Manager from Symantec 9
 - HPQFlash 14
 - HP Softpaq Download Manager 6
 - HP System Software Manager 6

Interface HP Client Management	6
Notificação Proativa de Alteração	13
Segurança para HP Business PC	7
Seleção de Assinante	13
suporte de software	24
Suporte HP	11
Tecnologia Intel vPro	11