Desktop Management-Handbuch

HP Business PCs

Desktop Management-Handbuch

HP Business PCs

Vierte Ausgabe (September 2009)

Dokumenten-Teilenummer: 581009-041

Allgemeines

Dieses Handbuch enthält Definitionen und Anleitungen zur Verwendung der Funktionen für Sicherheit und Manageability, die bei einigen Modellen voreingestellt sind.

VORSICHT! In dieser Form gekennzeichneter Text weist auf Verletzungs- oder Lebensgefahr bei Nichtbefolgen der Anleitungen hin.

ACHTUNG: In dieser Form gekennzeichneter Text weist auf die Gefahr von Hardwareschäden oder Datenverlust bei Nichtbefolgen der Anleitungen hin.

HINWEIS: In dieser Form gekennzeichneter Text weist auf wichtige Zusatzinformationen hin.

Inhaltsverzeichnis

1 Übersicht über Desktop Management

HP Client Management Solutions bietet auf Standards basierende Lösungen zur Verwaltung und Steuerung von Desktops, Workstations und Notebook-PCs in einer Netzwerkumgebung. HP war 1995 mit der Einführung der branchenweit ersten vollständig verwaltbaren Desktop-PCs ein Vorreiter im Bereich der Desktop Manageability. Die Manageability-Technologie von HP ist patentrechtlich geschützt. Seither ist HP führend bei der Entwicklung der Normen und Infrastruktur, die für eine effektive Nutzung, Verwaltung und Konfiguration von Desktops, Workstations und Notebooks erforderlich sind. Dabei entwickelt HP eigene Management-Software und arbeitet eng mit marktführenden Anbietern von Management-Software-Lösungen zusammen, um die Kompatibilität zwischen HP Client Management Solutions und diesen Produkten sicherzustellen. HP Client Management Solutions ist ein wichtiger Bestandteil der umfassenden HP Lösungen, mit denen sich die Betriebskosten senken und die Manageability Ihrer PCs während des gesamten Lebenszyklus gewährleisten lassen.

Die zentralen Funktionen und Merkmale des Desktop Management lauten:

- Erstkonfiguration und -einsatz
- Remote System Installation
- Software-Aktualisierung und-Management
- ROM-Flash
- Konfiguration optionaler Hardware-Geräte
- Bestandsüberwachung und Sicherheit
- Fehlermeldung und -beseitigung

HINWEIS: Die Unterstützung spezieller, in diesem Handbuch beschriebener Funktionen kann je nach Modell oder Softwareversion variieren.

2 Erstkonfiguration und -bereitstellung

Der Computer wird mit einem vorinstalliertem Systemsoftware-Image ausgeliefert. Nach einem kurzen Entpackvorgang ist der Computer einsatzbereit.

Möglicherweise ziehen Sie es vor, das vorinstallierte Software-Image durch eine benutzerdefinierte System- und Anwendungssoftware zu ersetzen. Es gibt mehrere Methoden zum Ersetzen eines benutzerdefinierten Software-Images. Folgende Methoden können verwendet werden:

- Installation zusätzlicher Software-Anwendungen nach dem Auspacken des vorinstallierten Software-Images.
- Verwendung von Software-Bereitstellungstools wie HP Client Automation Standard Edition, HP Client Automation Enterprise Edition (basierend auf Radia-Technologie), um die vorinstallierte Software durch ein benutzerdefiniertes Software-Image zu ersetzen.
- Verwendung eines Disk-Cloning-Vorgangs zum Kopieren des Inhalts einer Festplatte auf eine andere.

Welches Einsatzverfahren am besten geeignet ist, hängt von Ihrer IT-Umgebung und den damit verbundenen Prozessen ab.

Auf ROM basierendes Setup und ACPI-Hardware bieten weitere Unterstützung für die Wiederherstellung von Systemsoftware, Konfigurationsverwaltung, Fehlerbeseitigung und Energieverwaltung.

HP Client Automation Agent

Der von HP Client Automation Standard und Enterprise Editions verwendete Management-Agent ist auf dem Computer bereits vorhanden. Wenn er installiert wird, ermöglicht er die Kommunikation mit der HP Management-Konsole.

So installieren Sie den HP Client Automation Agent:

1. Klicken Sie auf **Start**.
2. Klicken Sie auf **Alle Programme**.
3. Klicken Sie auf **HP Manageability**.
4. Klicken Sie auf die **HP Management Agent Readme**-Datei der gewünschten Sprache.
5. Lesen und befolgen Sie die in der Readme-Datei enthaltenen Anleitungen, um den HP Client Automation Agent zu installieren.

HP Client Automation Agent ist eine zentrale Infrastrukturkomponente für die Aktivierung aller HP Client Automation-Lösungen. Ausführliche Informationen zu den anderen Infrastrukturkomponenten, die für

die Implementierung der HP Configuration Management-Lösungen erforderlich sind, finden Sie unter http://h20229.www2.hp.com/solutions/ascm/index.html.

HP Client Manager

HP Client Manager (HPCM) ist eine kostenfreie Lösung, die von Symantec entwickelt wurde und für alle unterstützten HP Business Desktop-, Notebook- und Workstation- und HP Blade-Modelle verfügbar ist. HPCM arbeitet mit HP spezifischen Tools wie System Software Manager, HP Instant Support Professional Edition und HP Client Management Interface, um die zentrale Verwaltung, Verfolgung und Überwachung sämtlicher unterstützter HP Hardware zu ermöglichen.

HP Client Manager 7.0 bietet eine völlig neue Portalseite, auf der Administratoren zentral die folgenden Verwaltungsaufgaben erfüllen können:

- Bestand
- Warnungen
- BIOS-Verwaltung
- Treiber-Updates
- Verwenden von HP Instant Support Health Scan und HP Instant Support Diagnostics
- Durchführung von Embedded Security-Aufgaben
- Anzeige der HP Trendübersicht der Systemwarnungen über die letzten drei bis sechs Monate
- Anzeige der allgemeinen Konformität unterstützter Computer mit HP Instant Support Health Scan und Diagnostics
- Anzeige der Übersicht der HP Computer – eine Übersicht der verschiedenen unterstützten Desktop-, Notebook-, Workstation- und HP Blade-PCs
- Anzeige von Warnungen: Bestand, Schwellenwert, Hardware-Zustand
- Berichte
- Administrative Aufgaben zur Aktualisierung HP spezifischer Tools

HPCM steht unter http://www.symantec.com/business/theme.jsp zum Download bereit. Klicken Sie dazu unter **Strategic Partner Products** auf **HP Client Manager**. Eine kostenlose unbegrenzte Lizenz ist ebenfalls auf der Download-Seite erhältlich.

Außerdem finden Sie unter http://www.symantec.com/connect Anleitungsvideos zum HPCM. Suchen Sie nach **HP Client Manager 7.0**, um Videos anzuzeigen, in denen verschiedene Aufgaben innerhalb von HPCM schrittweise beschrieben werden.

3 Remote System Installation

Remote System Installation ermöglicht das Starten und Einrichten des Systems unter Verwendung der auf einem Netzwerkserver befindlichen Software- und Konfigurationsinformationen, indem Preboot Execution Environment (PXE) gestartet wird. Die Funktion „Remote System Installation“ wird in der Regel zum Einrichten und Konfigurieren des Systems eingesetzt und kann für folgende Aufgaben verwendet werden:

- Formatieren einer Festplatte
- Verwenden eines Software-Images auf einem oder mehreren neuen PCs
- Remote-Aktualisierung des System-BIOS im Flash-ROM („Remote ROM Flash“ auf Seite 14)

  HINWEIS: Es besteht die Möglichkeit, das System-BIOS über das Betriebssystem Microsoft Windows zu aktualisieren.

- Konfigurieren der BIOS-Einstellungen des Systems

Zum Starten von Remote System Installation drücken Sie F12, sobald beim Hochfahren des Computers in der rechten unteren Ecke der HP Logoanzeige die Meldung **f12 = Network Service Boot** (Starten über Netzwerk) erscheint. Folgen Sie den Bildschirmanleitungen, um fortzufahren. Die standardmäßige Startreihenfolge ist eine BIOS-Konfigurationseinstellung, die jedoch so geändert werden kann, dass stets ein PXE-Startvorgang erfolgt.

4 Software-Aktualisierung und -Management

HP stellt eine Reihe von Tools für die Verwaltung und Aktualisierung von Software auf Desktops, Workstations und Notebooks zur Verfügung:

- HP Client Management Interface
- HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools Security Manager
- HP Client Automation Starter, Standard und Enterprise Editions
- HP Client Manager von Symantec
- Altiris Client Management Suite
- HP Client Catalog for Microsoft System Center & SMS Products
- Intel vPro-PCs mit Active Management Technology
- Verdiem Surveyor
- HP Proactive Change Notification
- HP Subscriber's Choice

HP Client Management Interface

Unabhängig von den Systemverwaltungstools, die Ihre IT-Abteilung verwendet, ist eine effiziente Verwaltung von Hardware und Software extrem wichtig, um Ihre IT-Kosten niedrig und das Unternehmen flexibel zu halten. Der IT-Administrator kann auf die HP Client Management Interface zugreifen, indem er einfache Skripte schreibt und diese Skripte in die gewünschte Management-Lösung integriert.

Mit HP Client Management Interface (HP CMI) können Sie neue HP Business PCs nahtlos in Ihre verwaltete IT-Umgebung integrieren. HP CMI bietet eine Schnittstelle für die einfache Integration von HP Business PCs mit gängigen Systemverwaltungstools (z. B. Microsoft Systems Management Server, IBM Tivoli Software und HP Operations) und intern entwickelten Verwaltungsprogrammen. Mit HP CMI können Tools und Anwendungen für die Systemverwaltung detaillierte Client-Inventardaten und Informationen über den Systemzustand abrufen sowie BIOS-Systemeinstellungen verwalten, indem sie direkt mit dem Client-Computer kommunizieren. Auf diese Weise lässt sich bei einem deutlich geringeren Bedarf an Agenten- oder Anschluss-Software eine effektive Integration erzielen.

HP Client Management Interface basiert auf Industriestandards wie Microsoft Windows Management Interface (MS WMI), Web-Based Enterprise Management (WBEM), System Management BIOS (SMBIOS) und Advanced Configuration and Power Interface (ACPI). HP CMI ist eine Basistechnologie, die bei HP Client Management Solutions eingesetzt wird. Mit HP CMI erhalten Sie die notwendige Flexibilität, um selbst zu entscheiden, wie Sie Ihre HP Client-Computer verwalten möchten.

In Kombination mit Systemverwaltungssoftware bietet HP Client Management Interface folgende Vorteile:

- Bereitstellung detaillierter Client-Inventardaten – Erfassung ausführlicher Informationen zu Prozessoren, Festplatten, Speicher, BIOS und Treibern einschließlich Messdaten wie Lüfterdrehzahl, Spannung und Temperatur.
- Bereitstellung von Informationen zum Festplattenstatus – Auswahl aus einer breiten Palette an Warnmeldungen zur Client-Hardware (z. B. Überhitzung, Lüfterausfall und Änderungen der Hardware-Konfiguration), die an die Systemverwaltungskonsole, die Anwendung oder den lokalen Client-Computer gesendet werden können. Dabei werden die Warnmeldungen bei Auftreten entsprechender Hardware-Ereignisse in Echtzeit übertragen.
- Verwaltung von BIOS-Systemeinstellungen – Durchführung von f10-Funktionen wie Einrichten und Ändern von BIOS-Kennwörtern sowie Remote-Definition und -Änderung der Startreihenfolge für beliebige Client-Systeme über die Systemverwaltungskonsole.

Weitere Informationen zu HP Client Management Interface finden Sie unter http://www.hp.com/go/hpcmi/.

HP SoftPaq Download Manager

HP SoftPaq Download Manager ist eine kostenlose, benutzerfreundliche Schnittstelle zum Auffinden und Herunterladen von Software-Updates für die HP Client-PC-Modelle in Ihrer Systemumgebung. Durch Angabe von Modell, Betriebssystem und Sprache können Sie schnell die benötigten Softpaqs auffinden, sortieren und auswählen. Zum Herunterladen von HP SoftPaq Download Manager besuchen Sie die Website http://www.hp.com/go/sdm.

HP System Software Manager

HP System Software Manager (SSM) ist ein kostenloses Dienstprogramm, das die automatische Remote-Bereitstellung von Gerätetreibern und BIOS-Updates für vernetzte HP Business PCs ermöglicht. SSM ermittelt im Hintergrund (d. h. ohne Benutzerinteraktion) die Treiber- und BIOS-Version auf dem vernetzten Client-System und vergleicht diese Daten mit Systemsoftware-SoftPaqs, die getestet und in einem zentralen Dateiarchiv abgelegt wurden. Danach ersetzt SSM veraltete Systemsoftware auf den vernetzten PCs automatisch durch die betreffende aktuelle Version aus dem Archiv. Da SSM absolut zuverlässig dafür sorgt, dass nur die richtigen SoftPaq-Updates auf die jeweiligen Client-Systemmodelle aufgespielt werden, können Administratoren mit diesem Dienstprogramm ihre Systemsoftware sicher und bequem auf dem neuesten Stand halten.

System Software Manager arbeitet reibungslos mit Tools für die Verteilung von Unternehmenssoftware zusammen, wie z. B. HP Client Automation-Lösungen, HP Client Manager from Symantec und Microsoft Systems Management Server (SMS). SSM ermöglicht die komfortable Verteilung von Updates, die vom Kunden generiert oder von Dritten bereitgestellt und im SSM-Format gepackt werden.

SSM kann kostenlos unter folgender Adresse heruntergeladen werden: http://www.hp.com/go/ssm.

HINWEIS: Remote-ROM-Flash wird von SSM derzeit nicht auf Systemen unterstützt, bei denen die Windows BitLocker-Laufwerksverschlüsselung aktiviert ist und die TPM-Messungen verwenden, um die BitLocker-Schlüssel zu schützen. Der Grund dafür ist, dass ein BIOS-Flash die vertrauenswürdige Signatur, die BitLocker für die Plattform erstellt hat, ungültig machen würde. Deaktivieren Sie BitLocker über die Gruppenrichtlinie, um das System-BIOS zu aktualisieren.

Sie können BitLocker-Unterstützung ohne TPM-Maßnahmen des BIOS aktivieren, um zu verhindern, dass die BitLocker-Schlüssel ungültig werden. HP empfiehlt, dass Sie ein sicheres Backup der BitLocker-Zugangsdaten aufbewahren, damit Sie notfalls schnell wiederherstellen können.

HP ProtectTools Security Manager

Die Sicherheitssoftware HP ProtectTools bietet Sicherheitsfunktionen, um den unbefugten Zugriff auf den Computer sowie auf Netzwerke und kritische Daten zu verhindern. Die folgenden Softwaremodule bieten erweiterte Sicherheitsfunktionen, auf die über HP ProtectTools Security Manager zugegriffen werden kann:

HP ProtectTools Security Manager ist die Konsole, über die auf alle anderen Module zugegriffen wird.

- Credential Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Privacy Manager für 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 für HP ProtectTools

HP ProtectTools bietet zwei Versionen, die verwendet werden können: HP ProtectTools Security Manager und HP ProtectTools Administrative Console. Die Administrator- sowie die Benutzerversion sind verfügbar im Menü **Start** > **Alle Programme**.

Die für Ihren Computer erhältlichen Softwaremodule hängen vom Computermodell ab. So steht das Softwaremodul Embedded Security for HP ProtectTools beispielsweise nur auf Computern zur Verfügung, auf denen der integrierte TPM-Sicherheits-Chip (Trusted Platform Module) installiert ist.

Die Module der HP ProtectTools-Software sind entweder vorinstalliert, auf der Festplatte vorhanden oder können von der HP Website heruntergeladen werden. Für bestimmte HP Pro Desktop-Modelle ist HP ProtectTools als Aftermarket-Option erhältlich. Weitere Informationen hierzu finden Sie unter http://www.hp.com/products/security.

HP Client Automation Starter und Standard Editions

HP Client Automation ist eine Lösung zur Verwaltung von Hardware und Software für Windows Vista-, Windows XP- und HP Thin Client-Umgebungen, die bedienerfreundlich und schnell einsetzbar ist und

gleichzeitig eine solide Grundlage für zukünftige Anforderungen bietet. Für diese Lösung sind zwei Ausgaben erhältlich:

- Die Starter Edition ist ein kostenloses Produkt zur Verwaltung von HP Desktops, Notebooks und Workstations. Sie bietet eine Hardware- und Software-Inventarfunktion, Fernbedienung, HP Alarmüberwachung, HP BIOS- und Treiber-Updates, Integration mit HP Protect Tools und zusätzlichen Support für Intel AMT. Die Starter Edition unterstützt außerdem den Einsatz und die Verwaltung von HP Thin Clients.
- Die im Handel erhältliche Standard Edition enthält alle Funktionen der Starter Edition und verfügt zusätzlich über Funktionen für den Einsatz und die Migration unter Windows, Patch-Verwaltung, Softwareverteilung und die Messung der Softwarenutzung.

HP Client Automation Starter und Standard Editions bieten einen Migrationspfad zu HP Client Automation Enterprise Edition (basierend auf Radia-Technologie) für die automatisierte Verwaltung großer, heterogener und sich ständig verändernder IT-Umgebungen.

Weitere Informationen zu HP Client Automation-Lösungen finden Sie unter http://www.hp.com/go/client.

HP Client Automation Enterprise Edition

HP Client Automation Enterprise Edition ist eine richtlinienbasierte Lösung, die es Administratoren ermöglicht, Software und Content auf heterogenen Client-Plattformen zu inventarisieren, einzusetzen und fortlaufend zu verwalten. Mit der HP Client Automation Enterprise Edition haben IT-Experten folgende Möglichkeiten:

- Automatisierung des gesamten Lebenszyklusverwaltungsprozesses von der Erkennung über den Einsatz und die fortlaufende Verwaltung bis hin zu Migration und Außerbetriebnahme
- Automatischer Einsatz sowie fortlaufende Verwaltung und Aufrechterhaltung einer gesamten Software-Umgebung (Betriebssysteme, Anwendungen, Patches, Einstellungen und Inhalte) im gewünschten Zustand
- Software-Verwaltung auf praktisch jedem Gerät, einschließlich Desktops, Workstations und Notebooks, in einer heterogenen, eigenständigen Infrastruktur
- Software-Verwaltung auf den meisten Betriebssystemen

HP Kunden berichten von erheblichen Einsparungen bei den IT-Kosten, kürzerer Time-to-Market für Software und Inhalte sowie einer deutlich höheren Produktivität und Zufriedenheit der Benutzer infolge des Einsatzes der ständigen Konfigurationsverwaltung.

Weitere Informationen zu HP Client Automation-Lösungen finden Sie unter http://www.hp.com/go/client.

HP Client Manager von Symantec

HP Client Manager von Symantec, entwickelt mit Altiris, ist für alle unterstützten HP Business Desktop-, Notebook- und Workstation-Modelle verfügbar. SSM ist in HP Client Manager integriert und ermöglicht die zentrale Verfolgung, Überwachung und Verwaltung der Hardwareaspekte von HP Client-Systemen.

HP Client Manager von Symantec bietet folgende Möglichkeiten:

- Bereitstellung nützlicher Hardware-Informationen zu CPU, Speicher, Videosystem und Sicherheitseinstellungen
- Überwachung des Systemzustands für die proaktive Behebung potenzieller Probleme
- Automatisches Aufspielen und Installieren von Treiber- und BIOS-Updates, ohne dass der Administrator tatsächlich vor Ort sein muss
- Fernkonfiguration von BIOS- und Sicherheitseinstellungen
- Automatisierung von Prozessen für eine schnelle Behebung von Hardwareproblemen

Enge Einbindung in HP Instant Support Tools für die schnellere Behebung von Hardwarefehlern

- Diagnostics – Remote-Ausführung und -Anzeige von Berichten zu HP Desktop-, Notebook- und Workstation-Modellen
- System Health Scan – Überprüft die installierten HP Client-Systeme auf bekannte Hardwareprobleme
- Active Chat – Stellt eine Verbindung zur HP Kundenunterstützung her
- HP Knowledgebase – Bietet eine Fülle von wertvollen Tipps und Informationen
- Automatischer SoftPaq-Abruf- und Bereitstellungsprozess für die schnelle Behebung von Hardwareproblemen
- Erkennung, Inventarisierung und Initialisierung von Systemen mit dem integrierten Sicherheitschip von HP ProtectTools
- Optionale Ausgabe von Warnmeldungen zum Systemzustand auf lokalem Client-System
- Protokollierung grundlegender Inventardaten für nicht von HP stammende Clients
- Einrichten und Konfigurieren des TPM-Sicherheitschip
- Zentrales Planen der Client-Sicherung und Wiederherstellung
- Zusätzliche Unterstützung für die Verwaltung von Intel AMT

Weitere Informationen zu HP Client Manager von Symantec finden Sie unter http://www.hp.com/go/clientmanager.

Altiris Client Management Suite

Altiris Client Management Suite ist eine benutzerfreundliche Softwareverwaltungslösung für Desktop-, Notebook- und Workstation-PCs, die den gesamten Lebenszyklus umfasst. Client Management Suite umfasst die folgenden Altiris Produkte:

- Inventory Solution
- Deployment Solution
- Software Delivery Solution
- Patch Management Solution
- Application Metering Solution

- Application Management Solution
- Carbon Copy Solution

Weitere Informationen zur Altiris Client Management Suite finden Sie unter http://www.symantec.com/business/client-management-suite.

HP Client Catalog for Microsoft System Center & SMS Products

Mit HP Client Catalog können IT-Mitarbeiter, die Microsoft Produkte verwenden, die Bereitstellung der HP Software-Updates (Softpaqs) auf HP Business PCs automatisieren. Die Katalogdatei enthält detaillierte Plattforminformationen zu HP Business Desktops, Notebooks und Workstations. Sie kann in Verbindung mit den benutzerdefinierten Inventar- und Update-Funktionen der Microsoft-Produkte verwendet werden, um automatisierte Treiber- und Patch-Updates für verwaltete HP Client-Computer bereitzustellen.

Von HP Client Catalog unterstützte Microsoft-Produkte:

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

Weitere Informationen zu HP Client Catalog for SMS finden Sie unter http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html.

Remote-Verwaltungstechnologie

Die Modelle umfassen entweder vPro-Technologie oder Standardtechnologie. Beide Technologien ermöglichen eine bessere Erkennung, Problembehebung und einen besseren Schutz der an das Netzwerk angeschlossenen Computerbestände. Beide Technologien ermöglichen die Verwaltung von PCs, unabhängig davon, ob sie eingeschaltet oder ausgeschaltet sind oder nicht mehr reagieren.

Die drei Formen der Remote-Verwaltung, die auf Business-Desktop-PCs verfügbar sind, sind ASF (Alert Standard Format), AMT (Intel Active Management Technology) und DASH (Desktop and Mobile Architecture for Systems Hardware).

Funktionen der Remote-Verwaltungstechnologie:

- Netzwerkerkennung
- Bereitstellung von Hardware-Inventardaten
- Überwachung des Plattformstatus
- Power Management – Ein/Aus, Leistungswechsel
- Ferndiagnose und -reparatur
  - Textkonsolenumleitung – ermöglicht die Steuerung des Remote-PCs während der Bootphase über die Konsole
  - Umleitung von Laufwerken – ermöglicht den Systemstart über ein Remote-Boot-Laufwerk, eine Diskette oder ein ISO-Image (die beiden Varianten sind IDE-Redirect (IDE-R) auf AMT-Plattformen und die Umleitung von USB-Geräten)

- Hardwarebasierte Isolierung und Wiederherstellung – Ermöglicht die Beschränkung bzw. Unterbindung des PC-Netzwerkzugriffs, falls eine verdächtige (Viren-)Aktivität entdeckt wird
- Ereignisverfolgung und –überwachung für Plattformen
- Integriertes Portal zur Webserververwaltung für Remotezugriff und -konfiguration
- Remote-Verwaltungstechnologien sind mit den HP Partnern für Verwaltungskonsolen integriert

HINWEIS: Nicht alle Funktionen sind auf allen Plattformen verfügbar.

Konfigurieren der Intel Management Engine

HINWEIS: Weitere Informationen zur Intel vPro-Technologie finden Sie unter http://www.intel.com/vpro.

HP spezifische Informationen zur Intel vPro-Technologie finden Sie in den White Papers unter http://www.hp.com/support. Wählen Sie dazu Ihr Land und Ihre Sprache aus. Wählen Sie dann **Informationen zu Support und Fehlerbehebung aufrufen**, und geben Sie Ihre Modellnummer ein. Drücken Sie anschließend die Eingabetaste. Klicken Sie in der Kategorie **Ressourcen** auf **Handbücher (Leitfäden, Zusatzinformationen, Ergänzungen usw.)**. Klicken Sie unter **Schnellaufruf von Handbüchern nach Kategorie...** auf **White Papers**.

Verfügbare Verwaltungstechnologien:

- AMT (einschließlich DASH 1.0)
- ASF
- DASH 1.1 (unter Verwendung einer Broadcom NIC)

ASF und AMT werden zwar beide unterstützt, dürfen jedoch nicht gleichzeitig konfiguriert sein.

So konfigurieren Sie Intel vPro-Systeme für AMT oder ASF:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Microsoft Windows auf **Start** > **Ausschalten** > **Neu starten**.
2. Drücken Sie sofort nach dem Einschalten des Computers die Tastenkombination Strg+P, bevor der Computer das Betriebssystem startet.

   HINWEIS: Wenn Sie Strg+P nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und erneut Strg+P drücken, bevor der Computer das Betriebssystem startet, damit das Dienstprogramm geöffnet wird.

Mit dieser Tastenkombination rufen Sie das Intel Management Engine BIOS Execution (MEBx)-Setup-Dienstprogramm auf. Es ermöglicht Ihnen die Konfiguration diverser Aspekte der Managementtechnologie. Verfügbare Konfigurationsoptionen:

- Hauptmenü
  - Intel ® ME Configuration (Intel ® ME-Konfiguration)
  - Intel ® AMT Configuration (Intel ® AMT-Konfiguration)
  - Change Intel ® ME Password (Intel ® ME-Kennwort ändern)
  - Exit (Beenden)
- Intel ® ME Platform Configuration (Intel ® ME-Plattformkonfiguration)
  - Intel ® ME State Control (Intel ® ME-Statuskontrolle) – Aktivieren/Deaktivieren
  - Intel ® ME Firmware Local Update (Lokales Intel ® ME-Firmware-Update) – Aktivieren/Deaktivieren
  - Intel ® ME Features Control (Intel ® ME-Funktionskontrolle)
  - Intel ® ME Power Control (Intel ® ME-Energiekontrolle)
- Intel ® AMT Configuration (Intel ® AMT-Konfiguration)
  - Host Name
  - TCP/IP
  - Provision Model (Bereitstellungsmodell) – Enterprise, SMB
  - Setup and Configuration (Setup und Konfiguration)
  - Un-Provision (Bereitstellung aufheben)
  - SOL/IDE-R – Aktivieren/Deaktivieren
  - Password Policy (Kennwortrichtlinie)
  - Secure Firmware Update (Sicheres Firmware-Update) – Aktivieren/Deaktivieren
  - Set PRTC (PRTC einstellen)
  - Idle Timeout (Leerlauf-Timeout)
- Change Intel ® ME Password (Intel ® ME-Kennwort ändern) – HP empfiehlt dringend, dieses Kennwort zu ändern. Das Standardkennwort ist **admin**.

Zur Remote-Verwaltung von AMT-Systemen muss der Administrator eine Remote-Konsole verwenden, die AMT unterstützt. Unternehmensverwaltungskonsolen sind von Anbietern wie HP, Altiris und Microsoft SMS erhältlich. Im SMB-Modus stellt der Client eine Webbrowser-Oberfläche zur Verfügung. Um auf diese Funktion zuzugreifen, öffnen Sie einen Browser auf einem anderen System des Netzwerks und geben `http://host_name:16992` ein, wobei `host_name` der Name des betreffenden Systems ist. Alternativ können Sie anstelle des Host-Namens auch die IP-Adresse des Systems eingeben.

So konfigurieren Sie Systeme mit einer DASH-fähigen NIC von Broadcam:

Die aktuellste Dokumentation finden Sie auf der Website http://www.hp.com unter **Support & Fehlerbehebung**. Wählen Sie dann Ihr Modell aus, und wählen Sie anschließend **Handbücher**, dann **White Papers**, die sich auf DASH oder die Broadcom-NIC beziehen.

Verdiem Surveyor

Verdiem Surveyor ist eine Softwarelösung zur Verwaltung der PC-Energiekosten. Surveyor ermittelt den Energieverbrauch jedes einzelnen PCs und gibt die Daten in einem Bericht aus. Darüber hinaus können Administratoren mit dieser Lösung die Energieeinstellungen von PCs steuern und bequem Energiesparstrategien in ihren Netzwerken implementieren. Ein HP SoftPaq mit Surveyor Agent kann von der HP Support-Website heruntergeladen und auf unterstützten, handelsüblichen Desktop-Modellen installiert werden. Wenden Sie sich an Ihren Ansprechpartner bei HP, wenn Sie Lizenzen für Surveyor zur Verwaltung von PCs benötigen.

HP Proactive Change Notification

Proactive Change Notification (Benachrichtigung über Produktänderungen) versendet auf Basis der Eintragungen auf der sicheren Website Subscriber's Choice unaufgefordert automatisch folgende Mails:

- Eine PCN-E-Mail (Product Change Notification), in der Sie bis zu 60 Tage im Voraus über Änderungen an der Hard- und Software informiert werden. Dieser Service wird für die meisten Computer und Server bereitgestellt, die in Unternehmen eingesetzt werden.
- Eine E-Mail mit Informationen, Ratschlägen und Hinweisen für Kunden, Sicherheitsmitteilungen und Treiber-Warnmeldungen. Auch dieser Service gilt für die meisten, in Unternehmen genutzten Computer und Server.

Durch die Erstellung Ihres persönlichen Profils wird gewährleistet, dass Sie nur Informationen erhalten, die für Ihre konkrete IT-Umgebung relevant sind. Weitere Informationen zu PCN und zur Erstellung eines persönlichen Profils finden Sie unter http://h30046.www3.hp.com/subhub.php

Subscriber’s Choice

Subscriber’s Choice ist ein Client-basierter HP Service.

Dabei stellt Ihnen HP ausgehend von Ihrem persönlichen Profil auf Sie abgestimmte Produkttipps, Artikel bzw. Treiber und Supportmeldungen/-benachrichtungen zur Verfügung.

In den von Subscriber’s Choice gesendeten E-Mails wird Ihnen mitgeteilt, dass die in Ihrem Profil angegebenen Informationen zum Abruf bereit stehen. Weitere Informationen zu Subscriber’s Choice und zur Erstellung eines persönlichen Profils finden Sie unter http://h30046.www3.hp.com/subhub.php.

Hinweis zur mitgelieferten Software

HP Business Desktop-, Notebook- oder Workstation-PCs werden nicht mehr mit den beiden Softwarepaketen Altiris Local Recovery und Dantz Retrospect ausgeliefert.

5 ROM-Flash

Das System-BIOS ist in einem programmierbaren Flash-ROM (Read Only Memory, Festwertspeicher) gespeichert. Damit der ROM nicht unbeabsichtigt aktualisiert oder überschrieben wird, können Sie in Computer Setup (f10) ein Setup-Kennwort einrichten. Dies ist wichtig, um die Betriebssicherheit des PCs sicherzustellen. Falls Sie das BIOS aktualisieren möchten, können Sie die neuesten BIOS-Images von der HP Website „Support und Treiber“ http://www.hp.com/support/files herunterladen.

△ **ACHTUNG:** Für maximalen ROM-Schutz müssen Sie ein Setup-Kennwort einrichten. Das Setup-Kennwort verhindert unbefugte ROM-Aktualisierungen. System Software Manager erlaubt dem Systemadministrator, das Setup-Kennwort auf einem oder mehreren PCs gleichzeitig einzurichten. Weitere Informationen hierzu finden Sie unter http://www.hp.com/go/ssm.

Remote ROM Flash

Remote ROM Flash ermöglicht dem Systemadministrator die sichere Aktualisierung des BIOS von entfernten HP Computern direkt über die zentrale Netzverwaltungskonsole. Indem der Systemadministrator diese Aufgabe auf mehreren Computern per Fernzugriff durchführen kann, lassen sich HP PC BIOS-Images über das Netzwerk konsistenter bereitstellen und besser überwachen. Dies führt außerdem zu höherer Produktivität und niedrigeren Total Cost of Ownership.

HINWEIS: Remote-ROM-Flash wird von SSM derzeit nicht auf Systemen unterstützt, bei denen die Windows BitLocker-Laufwerksverschlüsselung aktiviert ist und die TPM-Messungen verwenden, um die BitLocker-Schlüssel zu schützen. Der Grund dafür ist, dass ein BIOS-Flash die vertrauenswürdige Signatur, die BitLocker für die Plattform erstellt hat, ungültig machen würde. Deaktivieren Sie BitLocker über die Gruppenrichtlinie, um das System-BIOS zu aktualisieren.

Der Computer muss eingeschaltet sein oder über die Remote Wakeup-Funktion eingeschaltet werden, wenn Remote ROM Flash verwendet wird.

Weitere Informationen zu Remote-ROM-Flash finden Sie unter HP Client Manager Software oder System Software Manager unter http://www.hp.com/go/ssm/.

HPQFlash

Das HPQFlash Dienstprogramm dient zur lokalen Aktualisierung oder Wiederherstellung des System-BIOS einzelner PCs unter Windows.

Weitere Informationen zu HPQFlash finden Sie unter http://www.hp.com/support/files. Geben Sie die Modellnummer des Computers ein, wenn Sie dazu aufgefordert werden.

6 Boot Block Emergency Recovery Mode

Der Boot Block Emergency Recovery Mode (Startblock-Wiederherstellungsmodus) ermöglicht eine Wiederherstellung des Systems im unwahrscheinlichen Falle eines ROM-Flash-Fehlers. Dieser Fall kann z. B. bei einem Stromausfall während eines BIOS-Upgrades auftreten, in dessen Folge der ROM-Flash unvollständig und das System-BIOS nicht nutzbar wäre. Der Startblock (Boot Block) ist ein flash-geschützter Bereich des ROM-Speichers und enthält Code, mit dem bei jedem Einschalten des Systems die Gültigkeit des BIOS-System-Images überprüft wird.

- Wenn das BIOS-Image des Systems gültig ist, startet das System normal.
- Wenn das BIOS-Image des Systems ungültig ist, bietet ein ausfallsicheres Boot-Block-BIOS ausreichend Unterstützung, um Wechseldatenträger für BIOS-Image-Dateien zu suchen. Wenn eine geeignete Datei gefunden wird, wird sie automatisch in den ROM-Speicher übernommen.

Wenn ein ungültiges BIOS-Image des Systems festgestellt wird, leuchtet die rote Betriebs-LED achtmal im Abstand von jeweils einer Sekunde. Gleichzeitig ertönt achtmal ein Warnton. Wenn der Teil des System-ROMs mit dem Image des Grafik-Options-ROM nicht beschädigt ist, erscheint die Meldung **Boot Block Emergency Recovery Mode** (Startblock-Wiederherstellungsmodus).

Wenn Sie das System wiederherstellen möchten, nachdem es in den Boot Block Emergency Recovery Mode umgeschaltet wurde, führen Sie die folgenden Schritte aus:

1. Schalten Sie den Computer aus.
2. Legen Sie eine CD ein bzw. schließen Sie ein USB-Flash-Gerät mit der gewünschten BIOS-Image-Datei im Hauptverzeichnis an.

   HINWEIS: Das verwendete Medium muss mit dem FAT12-, FAT16- oder FAT32-Dateisystem formatiert worden sein.

3. Schalten Sie den Computer ein.

   Wenn kein angemessenes BIOS-Image gefunden wird, werden Sie aufgefordert, ein Medium mit einer BIOS-Image-Datei einzulegen.

   Wenn der ROM-Speicher erfolgreich programmiert werden kann, wird das System automatisch heruntergefahren.

4. Entfernen Sie das Wechselmedium, mit dem das BIOS aktualisiert wurde.
5. Schalten Sie den Computer anschließend wieder ein, oder starten Sie ihn neu.

HINWEIS: BitLocker hindert Windows Vista am Starten, wenn sich eine CD mit der BIOS-Image-Datei in einem optischen Laufwerk befindet. Wenn BitLocker aktiviert ist, entnehmen Sie diese CD, bevor Sie versuchen, Windows Vista zu starten.

7 Replizieren des Setups

Mit dem folgenden Verfahren kann der Systemadministrator ohne großen Aufwand eine Setup-Konfiguration auf andere Computer des gleichen Modells kopieren. Dies ermöglicht eine schnellere und konsistentere Konfiguration mehrerer Computer.

HINWEIS: Beide Verfahren erfordern ein Diskettenlaufwerk oder ein unterstütztes USB-Flash-Laufwerk.

HINWEIS: System Software Manager (SSM) kann verwendet werden, um Setup-Informationen des Computers über das Betriebssystem Microsoft Windows zu replizieren. Weitere Informationen finden Sie im SSM-Benutzerhandbuch unter http://www.hp.com/go/ssm.

Kopieren auf einen einzigen Computer

ACHTUNG: Setup-Konfigurationen sind modellspezifisch. Wenn Ausgangs- und Zielcomputer nicht zum selben Modell gehören, kann das Dateisystem beschädigt werden. So darf beispielsweise keinesfalls die Setup-Konfiguration eines dc7xxx PC auf einen dx7xxx PC kopiert werden.

1. Wählen Sie die zu kopierende Setup-Konfiguration aus. Schalten Sie den Computer aus. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Herunterfahren**.
2. Wenn Sie ein USB-Flash-Media-Gerät verwenden, schließen Sie es jetzt an einen USB-Port des Computers an.
3. Schalten Sie den Computer ein.
4. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, bevor das Betriebssystem startet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und vor dem Start des Betriebssystems erneut F10 drücken, damit das Dienstprogramm geöffnet wird.
5. Wenn Sie eine Diskette verwenden, legen Sie sie jetzt ein.
6. Klicken Sie auf **Datei** > **Replicated Setup** (Setup-Replikation) > **Save to Removable Media** (Auf Wechsellaufwerk speichern). Folgen Sie den Bildschirmanleitungen, um die Konfigurationsdiskette oder das USB-Flash-Media-Gerät zu erstellen.
7. Schalten Sie den zu konfigurierenden Computer aus, und legen Sie die Konfigurationsdiskette ein, bzw. schließen Sie das USB-Flash-Media-Gerät an.
8. Schalten Sie den Computer anschließend wieder ein.

9. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, bevor das Betriebssystem startet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

10. Klicken Sie auf **Datei** > **Replicated Setup** (Setup-Replikation) > **Restore from Removable Media** (Von Wechsellaufwerk wiederherstellen), und folgen Sie den Anleitungen auf dem Bildschirm.

11. Starten Sie den Computer neu, sobald die Konfiguration abgeschlossen ist.

Kopieren auf mehrere Computer

△ **ACHTUNG:** Setup-Konfigurationen sind modellspezifisch. Wenn Ausgangs- und Zielcomputer nicht zum selben Modell gehören, kann das Dateisystem beschädigt werden. So darf beispielsweise keinesfalls die Setup-Konfiguration eines dc7xxx PC auf einen dx7xxx PC kopiert werden.

Bei diesem Verfahren dauert die Erstellung der Konfigurationsdiskette bzw. des USB-Flash-Media-Geräts etwas länger. Die Konfiguration auf die Zielcomputer nimmt dagegen sehr viel weniger Zeit in Anspruch.

HINWEIS: Bei diesem Verfahren benötigen Sie eine bootfähige Diskette oder ein bootfähiges USB-Flash-Media-Gerät. Wenn Sie nicht über Windows XP verfügen, um eine bootfähige Diskette zu erstellen, verwenden Sie das Verfahren für das Kopieren der Setup-Konfiguration auf einen einzelnen Computer (siehe „Kopieren auf einen einzigen Computer“ auf Seite 16).

1. Erstellen Sie eine bootfähige Diskette oder ein entsprechendes USB-Flash-Media-Gerät. Siehe „Unterstütztes USB-Flash-Media-Gerät“ auf Seite 18 oder „Unterstütztes USB-Flash-Media-Gerät“ auf Seite 20.

   △ **ACHTUNG:** Nicht alle Computer lassen sich von einem USB-Flash-Media-Gerät starten. Wenn das USB-Gerät in der standardmäßigen Startreihenfolge im Dienstprogramm „Computer Setup (f10) Utility“ vor dem Festplattenlaufwerk aufgelistet ist, kann der Computer von einem USB-Flash-Media-Gerät gestartet werden. Andernfalls muss eine bootfähige Diskette verwendet werden.

2. Wählen Sie die zu kopierende Setup-Konfiguration aus. Schalten Sie den Computer aus. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Herunterfahren**.

3. Wenn Sie ein USB-Flash-Media-Gerät verwenden, schließen Sie es jetzt an einen USB-Port des Computers an.

4. Schalten Sie den Computer ein.

5. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, bevor das Betriebssystem startet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und vor dem Start des Betriebssystems erneut F10 drücken, damit das Dienstprogramm geöffnet wird.

6. Wenn Sie eine Diskette verwenden, legen Sie sie jetzt ein.

7. Klicken Sie auf **Datei** > **Replicated Setup** (Setup-Replikation) > **Save to Removable Media** (Auf Wechsellaufwerk speichern). Folgen Sie den Bildschirmanleitungen, um die Konfigurationsdiskette oder das USB-Flash-Media-Gerät zu erstellen.

8. Laden Sie ein BIOS-Dienstprogramm für das Replizieren der Setup-Konfiguration (repset.exe) herunter, und kopieren Sie es auf die Konfigurationsdiskette bzw. das USB-Flash-Media-Gerät. Um das Dienstprogramm zu abzurufen, gehen Sie zu http://welcome.hp.com/country/us/en/support.html, und geben Sie die Modellnummer des betreffenden Computers ein.

9. Erzeugen Sie auf der Konfigurationsdiskette bzw. dem USB-Flash-Media-Gerät eine autoexec.bat-Datei mit dem folgenden Befehl:

   ```
   repset.exe
   ```

10. Schalten Sie den zu konfigurierenden Computer aus. Legen Sie die Konfigurationsdiskette ein, bzw. schließen Sie das USB-Flash-Media-Gerät an, und schalten Sie den Computer anschließend wieder ein. Das Konfigurationsdienstprogramm wird automatisch ausgeführt.

11. Starten Sie den Computer neu, sobald die Konfiguration abgeschlossen ist.

Erstellen eines bootfähigen Geräts

Unterstütztes USB-Flash-Media-Gerät

Unterstützte Geräte verfügen über ein vorinstalliertes Image, mit dem sie sich schnell und einfach als bootfähige Geräte erstellen lassen. Alle HP oder Compaq sowie die meisten anderen USB-Flash-Media-Geräte sind mit diesem vorinstallierten Image ausgestattet. Wenn das betreffende Gerät nicht über ein derartiges Image verfügt, folgen Sie den Anleitungen weiter unten in diesem Abschnitt (siehe „Unterstütztes USB-Flash-Media-Gerät“ auf Seite 20).

Zum Erstellen einer bootfähigen Diskette oder eines entsprechenden USB-Flash-Media-Geräts wird Folgendes benötigt:

- ein unterstütztes USB-Flash-Media-Gerät
- eine bootfähige DOS-Diskette mit den Programmen FDISK und SYS (falls SYS nicht vorhanden ist, kann FORMAT verwendet werden; in diesem Fall gehen jedoch alle auf dem USB-Flash-Media-Gerät vorhandenen Dateien verloren)
- ein PC, der sich von einem USB-Flash-Media-Gerät starten lässt

△ **ACHTUNG:** Einige ältere PCs lassen sich unter Umständen nicht von einem USB-Flash-Media-Gerät starten. Wenn das USB-Gerät in der standardmäßigen Startreihenfolge im Dienstprogramm „Computer Setup (f10) Utility“ vor dem Festplattenlaufwerk aufgelistet ist, kann der Computer von einem USB-Flash-Media-Gerät gestartet werden. Andernfalls muss eine bootfähige Diskette verwendet werden.

1. Schalten Sie den Computer aus.

2. Verbinden Sie das USB-Flash-Media-Gerät mit einem der USB-Ports des Computers, und entfernen Sie alle anderen USB-Speichergeräte mit Ausnahme der USB-Diskettenlaufwerke.

3. Legen Sie eine bootfähige DOS-Diskette mit FDISK.COM und SYS.COM oder FORMAT.COM in ein Diskettenlaufwerk ein, und schalten Sie dann den Computer ein, um von der DOS-Diskette zu starten.

4. Führen Sie FDISK über die Eingabeaufforderung **A:** aus, indem Sie `FDISK` eingeben und die Eingabetaste drücken. Klicken Sie bei Aufforderung auf **Ja** (**J**), um Unterstützung für große Festplatten zu aktivieren.

5. Geben Sie den Wert [5] ein, um die Laufwerke des Systems anzeigen zu lassen. Das USB-Flash-Media-Gerät ist das Laufwerk, das am ehesten mit der Größe eines der aufgelisteten Laufwerke

übereinstimmt. Meistens ist es das letzte Laufwerk in der Liste. Achten Sie dabei auf den Laufwerksbuchstaben.

Laufwerk des USB-Flash-Media-Geräts: _____

△ **ACHTUNG:** Wenn keines der angezeigten Laufwerke mit dem USB-Flash-Media-Gerät übereinstimmt, fahren Sie nicht fort, da es andernfalls zu Datenverlust kommen kann. Überprüfen Sie alle USB-Ports auf weitere Speichergeräte. Falls weitere Geräte vorhanden sein sollten, entfernen Sie sie, starten den Computer neu und fahren mit Schritt 4 fort. Wenn keine Geräte vorhanden sind, unterstützt das System entweder das betreffende USB-Flash-Media-Gerät nicht, oder das Gerät ist defekt. Versuchen Sie in diesem Fall NICHT weiter, das USB-Flash-Media-Gerät bootfähig zu machen.

6. Verlassen Sie FDISK durch Drücken der Esc-Taste, um zur Eingabeaufforderung **A:** zurückzukehren.

7. Wenn Ihre bootfähige DOS-Diskette SYS.COM enthält, fahren Sie mit Schritt 8 fort. Wenn dies nicht der Fall ist, fahren Sie mit Schritt 9 fort.

8. Geben Sie an der Eingabeaufforderung **A:** `SYS x:` ein, wobei x für den oben erwähnten Laufwerksbuchstaben steht.

△ **ACHTUNG:** Stellen Sie sicher, dass Sie den korrekten Laufwerksbuchstaben für das USB-Flash-Media-Gerät eingegeben haben.

Nach der Übertragung der Systemdateien kehrt SYS zur Eingabeaufforderung **A:** zurück. Fahren Sie mit Schritt 13 fort.

9. Kopieren Sie alle Dateien, die Sie behalten möchten, von Ihrem UBS-Flash-Media-Gerät in ein temporäres Verzeichnis auf einem anderen Laufwerk (z. B. auf dem internen Festplattenlaufwerk des Systems).

10. Geben Sie an der Eingabeaufforderung **A:** `FORMAT /S X:` ein, wobei `X` für den oben erwähnten Laufwerksbuchstaben steht.

△ **ACHTUNG:** Stellen Sie sicher, dass Sie den korrekten Laufwerksbuchstaben für das USB-Flash-Media-Gerät eingegeben haben.

FORMAT zeigt eine oder mehrere Meldungen an und fragt Sie jedes Mal, ob Sie fortfahren möchten. Geben Sie jedes Mal `J` ein. FORMAT formatiert das USB-Flash-Media-Gerät, fügt die Systemdateien hinzu und fordert Sie zur Eingabe der Datenträgerkennung auf.

11. Falls Sie keine Kennung eingeben möchten, drücken Sie die Eingabetaste; andernfalls geben Sie die gewünschte Datenträgerkennung ein.

12. Kopieren Sie die in Schritt 9 gesicherten Dateien auf das USB-Flash-Media-Gerät.

13. Nehmen Sie die Diskette aus dem Laufwerk, und starten Sie den Computer neu. Der Computer startet von dem USB-Flash-Media-Gerät als Laufwerk C.

HINWEIS: Die standardmäßige Startreihenfolge variiert von Computer zu Computer und kann mit Computer Setup (f10) Utility geändert werden.

Wenn Sie eine DOS-Version unter Windows 9x verwendet haben, wird unter Umständen kurzfristig der Windows Anmeldebildschirm angezeigt. Wenn dieser Bildschirm nicht erscheinen soll, fügen Sie dem Hauptverzeichnis des USB-Flash-Media-Geräts eine Datei mit Null-Länge und der Bezeichnung LOGO.SYS hinzu.

Kehren Sie zu „Kopieren auf mehrere Computer“ auf Seite 17 zurück.

Unterstütztes USB-Flash-Media-Gerät

Zum Erstellen einer bootfähigen Diskette oder eines entsprechenden USB-Flash-Media-Geräts wird Folgendes benötigt:

- ein USB-Flash-Media-Gerät
- eine bootfähige DOS-Diskette mit den Programmen FDISK und SYS (falls SYS nicht vorhanden ist, kann FORMAT verwendet werden; in diesem Fall gehen jedoch alle auf dem USB-Flash-Media-Gerät vorhandenen Dateien verloren)
- ein PC, der sich von einem USB-Flash-Media-Gerät starten lässt

△ **ACHTUNG:** Einige ältere PCs lassen sich unter Umständen nicht von einem USB-Flash-Media-Gerät starten. Wenn das USB-Gerät in der standardmäßigen Startreihenfolge im Dienstprogramm „Computer Setup (f10) Utility“ vor dem Festplattenlaufwerk aufgelistet ist, kann der Computer von einem USB-Flash-Media-Gerät gestartet werden. Andernfalls muss eine bootfähige Diskette verwendet werden.

1. Wenn das System über PCI-Karten mit angeschlossenen SCSI-, ATA RAID- oder SATA-Laufwerken verfügt, schalten Sie den Computer aus und ziehen das Netzkabel.

   △ **ACHTUNG:** Das Netzkabel muss UNBEDINGT gezogen werden.

2. Öffnen Sie die Gehäuseabdeckung, und entfernen Sie die PCI-Karten.
3. Verbinden Sie das USB-Flash-Media-Gerät mit einem der USB-Ports des Computers, und entfernen Sie alle anderen USB-Speichergeräte mit Ausnahme der USB-Diskettenlaufwerke. Bringen Sie die Gehäuseabdeckung wieder an.
4. Stecken Sie das Netzkabel ein, und schalten Sie den Computer ein.
5. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, bevor das Betriebssystem startet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und vor dem Start des Betriebssystems erneut F10 drücken, damit das Dienstprogramm geöffnet wird.

6. Wechseln Sie zu **Erweitert** > **PCI Devices** (PCI-Geräte), um sowohl den PATA- als auch den SATA-Controller zu deaktivieren. Notieren Sie sich bei der Deaktivierung des SATA-Controllers dessen IRQ-Zuordnung, da Sie sie später wieder zuweisen müssen. Verlassen Sie das Setup-Programm, und bestätigen Sie dabei die vorgenommenen Änderungen.

   SATA-IRQ: _____

7. Legen Sie eine bootfähige DOS-Diskette mit FDISK.COM und SYS.COM oder FORMAT.COM in ein Diskettenlaufwerk ein, und schalten Sie dann den Computer ein, um von der DOS-Diskette zu starten.
8. Führen Sie FDISK aus, und löschen Sie alle vorhandenen Partitionen auf dem USB-Flash-Media-Gerät. Erzeugen Sie eine neue Partition, und markieren Sie sie als die aktive Partition. Beenden Sie FDISK, indem Sie die Esc-Taste drücken.
9. Wenn das System beim Beenden von FDISK nicht automatisch neu gestartet wurde, drücken Sie Strg+Alt+Entf, um von der DOS-Diskette zu starten.

10. Geben Sie an der Eingabeaufforderung **A:** `FORMAT C: /S` ein, und drücken Sie dann die Eingabetaste. FORMAT formatiert das USB-Flash-Media-Gerät, kopiert die Systemdateien und fordert Sie zur Eingabe einer Datenträgerkennung auf.

11. Falls Sie keine Kennung eingeben möchten, drücken Sie die Eingabetaste; andernfalls geben Sie die gewünschte Datenträgerkennung ein.

12. Schalten Sie den Computer aus, und ziehen Sie das Netzkabel. Öffnen Sie die Gehäuseabdeckung, und setzen Sie die PCI-Karten wieder ein. Bringen Sie die Gehäuseabdeckung wieder an.

13. Stecken Sie das Netzkabel ein, nehmen Sie die Diskette aus dem Laufwerk, und schalten Sie dann den Computer wieder ein.

14. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, bevor das Betriebssystem startet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

15. Wechseln Sie zu **Erweitert** > **PCI Devices** (PCI-Geräte), und aktivieren Sie die PATA- und SATA-Controller, die in Schritt 6 deaktiviert wurden. Stellen Sie die ursprüngliche IRQ-Zuordnung für den SATA-Controller wieder her.

16. Speichern Sie die vorgenommenen Änderungen, und verlassen Sie das Programm. Der Computer startet von dem USB-Flash-Media-Gerät als Laufwerk C.

HINWEIS: Die standardmäßige Startreihenfolge ist von Computer zu Computer verschieden und kann in Computer Setup (f10) geändert werden. Weitere Informationen finden Sie im Dokument *Computer Setup (f10) Utility* .

Wenn Sie eine DOS-Version unter Windows 9x verwendet haben, wird unter Umständen kurzfristig der Windows Anmeldebildschirm angezeigt. Wenn dieser Bildschirm nicht erscheinen soll, fügen Sie dem Hauptverzeichnis des USB-Flash-Media-Geräts eine Datei mit Null-Länge und der Bezeichnung LOGO.SYS hinzu.

Kehren Sie zu „Kopieren auf mehrere Computer“ auf Seite 17 zurück.

8 Dual-State-Netzschalter

Bei aktivierter ACPI-Funktion (Advanced Configuration and Power Interface) übernimmt der Netzschalter entweder die Funktion des Ein-/Aus-Schalters oder der Standby-Taste. In der Funktion als Standby-Taste unterbricht er die Stromzufuhr nicht, sondern schaltet den Computer auf einen geringen Stromverbrauch um. Dadurch können Sie schnell in den Energiesparmodus schalten, ohne die Anwendungen schließen zu müssen; außerdem können Sie ohne Datenverlust schnell in den vorherigen Betriebszustand zurückkehren.

So ändern Sie die Konfiguration des Netzschalters:

1. Klicken Sie mit der linken Maustaste auf **Start**, **Systemsteuerung** > **Energieoptionen**.
2. Öffnen Sie unter **Eigenschaften von Energieoptionen** die Registerkarte **Erweitert**.
3. Wählen Sie im Abschnitt **Netzschaltervorgänge** die Option **In den Standby-Modus wechseln** aus.

Nachdem Sie den Netzschalter als Standby-Taste konfiguriert haben, können Sie das System mit dem Schalter auf einen sehr geringen Stromverbrauch (Standby-Modus) umschalten. Durch erneutes Drücken der Standby-Taste schalten Sie aus dem Standby-Modus auf Normalbetrieb um. Wenn Sie die Stromzufuhr ganz unterbrechen wollen, halten Sie den Netzschalter vier Sekunden lang gedrückt.

△ **ACHTUNG:** Schalten Sie den Computer nur über den Netzschalter aus, wenn das System nicht mehr reagiert. Fahren Sie den Computer ansonsten über die Optionen des Betriebssystems herunter, da ansonsten die Gefahr der Beschädigung oder des Verlusts von Daten auf der Festplatte besteht.

9 HP Website-Unterstützung

Die HP Techniker testen die von HP und Drittanbietern entwickelte Software nach strengen Kriterien und entwickeln auf das jeweilige Betriebssystem zugeschnittene Support-Software, um so eine optimale Leistung, Kompatibilität und Zuverlässigkeit von HP Computern zu gewährleisten.

Wenn Sie ein neues oder überarbeitetes Betriebssystem auf Ihrem Computer installieren, sollten Sie unbedingt auch die für das jeweilige Betriebssystem entwickelte Support-Software installieren. Wenn Sie mit einer anderen als der vorinstallierten Version von Microsoft Windows arbeiten möchten, müssen Sie die entsprechenden Gerätetreiber und Dienstprogramme installieren. Nur so ist sichergestellt, dass alle Funktionen unterstützt werden und einwandfrei arbeiten.

HP erleichtert das Auffinden und den Zugriff auf die neueste Support-Software sowie deren Prüfung und Installation. Die Software steht unter http://www.hp.com/support zum Download bereit.

Die Website enthält die neuesten Gerätetreiber, Dienstprogramme und Flash-ROM-Images, die zur Ausführung des aktuellen Microsoft Windows Betriebssystems auf Ihrem HP Computer erforderlich sind.

10 Branchenstandards

HP Management Lösungen können in andere Systemverwaltungslösungen integriert werden. Unter anderem werden die folgenden Branchenstandards beachtet:

- Web-Based Enterprise Management (WBEM)
- Windows Management Interface (WMI)
- Wake-on-LAN-Technologie
- ACPI
- SMBIOS
- PXE (Pre-boot Execution)-Unterstützung

11 Bestandsüberwachung und Sicherheit

Die auf dem Computer vorinstallierten Funktionen zur Bestandsüberwachung stellen Ihnen wichtige Informationen bereit, die über HP Systems Insight Manager, HP Client Manager, HP Configuration Management Solution und HP Client Configuration Manager sowie andere Management-Anwendungen verwaltet werden können. Durch die nahtlose und automatische Integration in diese Produkte können Sie das Management-Tool auswählen, das für Ihre Umgebung am besten geeignet ist, ohne Ihre vorhandenen Investitionen in entsprechende Tools zu gefährden.

Darüber hinaus bietet HP mehrere Lösungen zur Steuerung des Zugriffs auf wichtige Komponenten und Daten an. HP Embedded Security for ProtectTools unterbindet (sofern installiert) den unbefugten Zugriff auf Daten, überprüft die Systemintegrität und authentifiziert Fremdbenutzer, die versuchen, auf das System zuzugreifen. Weitere Informationen finden Sie im *HP ProtectTools Security Manager-Handbuch* unter http://www.hp.com/products/security. Sicherheitsfunktionen wie HP Embedded Security for ProtectTools, Smart Cover Sensor und Smart Cover Lock, die auf einigen Modellen verfügbar sind, verhindern den unbefugten Zugriff auf interne Bestandteile des PCs. Durch die Deaktivierung von parallelen und seriellen Anschlüssen sowie USB-Ports oder durch die Deaktivierung der Bootfähigkeit von Wechsellaufwerken können Sie wertvolle Datenbestände schützen. Memory Change- und Smart Cover Sensor-Warnmeldungen können automatisch an die jeweiligen Systemverwaltungsprogramme weitergeleitet werden, um darauf aufmerksam zu machen, dass sich eine unbefugte Person Zugang zu den internen Computerkomponenten verschaffen möchte.

HINWEIS: HP Embedded Security for ProtectTools, der Smart Cover Sensor und das Smart Cover Lock sind optionale Merkmale, die nur für bestimmte Modelle zur Verfügung stehen.

Verwenden Sie die folgenden Dienstprogramme zur Verwaltung der Sicherheitseinstellungen auf HP Computern:

- Lokal, über Computer Setup. Zusätzliche Informationen und Anleitungen zur Verwendung von Computer Setup finden Sie im *Computer Setup (f10) Utility-Handbuch*, das im Lieferumfang des Computers enthalten ist.
- Remote, mit HP Client Manager von Symantec, HP Client Automation oder System Software Manager. Diese Software ermöglicht den sicheren, einheitlichen Einsatz und die Steuerung von Sicherheitseinstellungen.

Die folgende Tabelle und die zugehörigen Abschnitte beziehen sich auf die lokale Verwaltung von Sicherheitsfunktionen über Computer Setup Utility (f10).

Tabelle 11-1 Sicherheitsfunktionen – Übersicht

Option	Beschreibung
Setup Password (Setup-Kennwort)	Ermöglicht die Einrichtung und Aktivierung des (Administrator-)Setup-Kennworts. **HINWEIS:** Wenn ein Setup-Kennwort eingerichtet wurde, ist seine Eingabe erforderlich, um die Optionen für Computer Setup zu ändern, den ROM-Speicher zu aktualisieren oder Änderungen an bestimmten Plug-and-Play-Einstellungen unter Windows vorzunehmen.

Tabelle 11-1 Sicherheitsfunktionen – Übersicht (Fortsetzung)

Power-On Password (Kennwort für den Systemstart)	Ermöglicht die Einrichtung und Aktivierung des Kennworts für den Systemstart. Sie werden zur Eingabe eines Systemstart-Kennworts aufgefordert, wenn das System aus- und wieder eingeschaltet wurde. Bei Eingabe des falschen Kennworts startet das System nicht. **HINWEIS:** Beim Warmstart, z. B. Strg+Alt+Löschen, oder beim **Neustart von Windows** wird die Kennworteingabe nur bei entsprechender Einstellung unter **Kennwort-Optionen** angezeigt (siehe unten).
Password Options (Kennwortoptionen) (Diese Auswahlmöglichkeit steht nur zur Verfügung, wenn ein Systemstart- oder Setup-Kennwort eingerichtet wurde.)	Ermöglicht die folgenden Einstellungen: • Sperren von älteren Ressourcen (falls ein Setup-Kennwort eingerichtet wurde) • Aktivieren bzw. Deaktivieren des Netzwerk-Servermodus (falls ein Systemstart-Kennwort eingerichtet wurde) • Ermöglicht Ihnen festzulegen, ob für Warmstarts mit Strg+Alt+Entf ein Kennwort erforderlich ist (falls ein Systemstart-Kennwort eingerichtet wurde) • Aktivieren bzw. Deaktivieren von **Setup Browse Mode** (Setup durchsuchen). Diese Option ist nur verfügbar, wenn ein Setup-Kennwort eingerichtet wurde. Sie ermöglicht die Anzeige – jedoch nicht die Änderung – der f10 Setup-Optionen ohne Eingabe des Setup-Kennworts. • Aktivieren bzw. Deaktivieren von **Stringent Password** (Kennwort für hohe Sicherheit). Diese Option (nur verfügbar, wenn ein Systemstart-Kennwort eingerichtet wurde) überspringt den Kennwort-Jumper, um das Systemstartkennwort zu deaktivieren. Weitere Informationen finden Sie im Handbuch *Desktop Management*.
Smart Cover (bestimmte Modelle)	Ermöglicht die folgenden Einstellungen: • Sperren/Entsperren des Cover Lock (Gehäusesperre). • Die folgenden Optionen stehen für den Cover Removal Sensor zur Auswahl: **Disable/Notify User/Setup Password** (Deaktivieren/Benutzer benachrichtigen/Setup-Kennwort). **HINWEIS:** Mit *Notify User* (Benutzer benachrichtigen) wird der Benutzer benachrichtigt, falls der Sensor erkennt, dass die Abdeckung entfernt wurde. Mit *Setup Password* (Setup-Kennwort) wird festgelegt, dass zum Starten des Computers das Setup-Kennwort eingegeben werden muss, falls der Sensor erkannt hat, dass die Abdeckung entfernt wurde. Diese Funktion wird nur bei bestimmten Modellen unterstützt.
Device Security (Gerätesicherheit)	Ermöglicht die Einstellung von **Device Available/Device Hidden** (Gerät verfügbar/Gerät verborgen) für: • Serielle Schnittstellen • Parallele Schnittstelle • USB-Anschlüsse hinten • USB-Ports vorne • Interne USB-Anschlüsse • Audiosystem • Netzwerk-Controller (bestimmte Modelle) • Legacy Diskette (Älteres Diskettenlaufwerk) • Embedded Security-Chip (bestimmte Modelle) • SATA0 • SATA1 (bestimmte Modelle)

Tabelle 11-1 Sicherheitsfunktionen – Übersicht (Fortsetzung)

	• SATA2 (bestimmte Modelle) • SATA3 (bestimmte Modelle) • eSATA (bestimmte Modelle)
LoJack für HP ProtectTools	Ermöglicht die Remote-Steuerung, -Verwaltung und –Verfolgung Ihres Computers. Nach der Aktivierung wird LoJack Pro für HP ProtectTools vom Absolute Software-Kundencenter aus konfiguriert. Vom Kundencenter aus kann der Administrator die Überwachung oder Verwaltung des PCs durch LoJack für HP ProtectTools konfigurieren. Geht das System verloren oder wird es gestohlen, kann das Kundencenter den zuständigen Stellen vor Ort helfen, den Computer aufzufinden. Bei entsprechender Konfiguration kann LoJack Pro auch weiterhin aktiv sein, wenn die Festplatte gelöscht oder ersetzt wurde.
Network Service Boot (Starten über Netzwerk)	Ermöglicht das Aktivieren bzw. Deaktivieren der Funktion, mit der der Computer mit einem Betriebssystem gestartet werden kann, das auf einem Netzwerkserver installiert ist. (Diese Funktion steht nur für NIC-Modelle zur Verfügung. Der Netzwerk-Controller muss entweder eine PCI-Erweiterungskarte sein oder er muss auf der Systemplatine integriert sein.)
System IDs (System-IDs)	Ermöglicht die folgenden Einstellungen: • Bestandskennung (18-Byte-Kennung), eine Eigentümerkennung, die das Unternehmen dem betreffenden Computer zugeordnet hat. • Eigentümerkennung (80-Byte-Kennung), die während des POST angezeigt wird. • Seriennummer auf dem Gehäuse oder UUID-Nummer (Universal Unique Identifier). Die UUID kann nur geändert werden, wenn die aktuelle Seriennummer des Gehäuses ungültig ist. (Diese Nummern werden in der Regel im Werk vergeben und dienen zur eindeutigen Identifizierung des Systems.) • Landesspezifische Tastatureinstellungen (z. B. Englisch oder Deutsch) für die Eingabe der System-ID.
DriveLock Security (DriveLock-Sicherheitsfunktion)	Ermöglicht die Zuweisung oder Änderung eines Master- oder Benutzerkennworts für Festplatten. Bei Aktivierung dieser Funktion wird der Benutzer dazu aufgefordert, während des POST eines der DriveLock-Kennwörter einzugeben. Wenn kein korrektes Kennwort eingegeben wird, kann so lange nicht auf die Festplatte zugegriffen werden, bis bei nachfolgenden Kaltstarts eines der Kennwörter erfolgreich eingegeben wurde. **HINWEIS:** Diese Auswahl steht nur dann zur Verfügung, wenn wenigstens ein Laufwerk mit DriveLock-Unterstützung an das System angeschlossen ist.
Setup Security Level (Setup-Schutzstufe)	Ermöglicht dem Administrator, den Benutzern einen beschränkten Zugriff zuzuweisen, mit dem sie bestimmte Setup-Optionen auch ohne Eingabe des Setup-Kennworts ändern können. Auf diese Weise kann der Administrator wichtige Setup-Optionen flexibel schützen und den Benutzern gleichzeitig die Anzeige von Systemeinstellungen und die Konfiguration weniger wichtiger Optionen ermöglichen. Dabei vergibt der Administrator über das Menü **Setup Security Level** (Setup-Schutzstufe) spezifische Zugriffsrechte für einzelne Setup-Optionen. Standardmäßig ist für die Änderung aller Setup-Optionen das Setup-Kennwort erforderlich; d. h. der Benutzer muss während des POST das korrekte Setup-Kennwort eingeben, um eine Änderung vornehmen zu können. Der Administrator kann einzelne Optionen auf **None** (Ohne) setzen, so dass der Benutzer diese Optionen auch ohne Eingabe des korrekten Kennworts ändern kann. Falls die Eingabe des Kennworts für den Systemstart aktiviert wurde, lautet die Option **Power-On Password** (Systemstart-Kennwort). **HINWEIS:** Damit auch ohne Eingabe des Setup-Kennworts ein Zugriff auf die Setup-Konfiguration möglich ist, muss **Setup Browse Mode** (Setup durchsuchen) auf **Enable** (Aktivieren) gesetzt worden sein.
System Security (Systemsicherheit) (nur bestimmte Modelle:	Data Execution Prevention (Datenausführung unterbinden) (bestimmte Modelle) (Aktivieren/ Deaktivieren) – Schließt Lücken bei der Betriebssystemsicherheit.

Tabelle 11-1 Sicherheitsfunktionen – Übersicht (Fortsetzung)

Optionen hängen von der Hardware ab)	Virtualization Technology (Virtualisierungstechnologie) (bestimmte Modelle) (Aktivieren/Deaktivieren) – Steuert die Virtualisierungsfunktionen des Prozessors. Zum Ändern dieser Einstellung muss der Computer ausgeschaltet und anschließend wieder eingeschaltet werden. Virtualization Technology Directed I/O (Virtualisierungstechnologie E/A geleitet) (bestimmte Modelle) (Aktivieren/Deaktivieren) – Steuert die Funktionen zur Neuzuordnung der Virtualisierungsfunktionen des Chipsatzes. Zum Ändern dieser Einstellung muss der Computer ausgeschaltet und anschließend wieder eingeschaltet werden. Trusted Execution Technology (Vertrauenswürdige Ausführungstechnologie) (bestimmte Modelle) (Aktivieren/Deaktivieren) – Steuert die zugrunde liegenden Prozessor- und Chipsatz-Funktionen, die zur Unterstützung einer virtuellen Anwendung erforderlich sind. Zum Ändern dieser Einstellung muss der Computer ausgeschaltet und anschließend wieder eingeschaltet werden. Aktivieren Sie die folgenden Funktionen, um diese Option zu nutzen: ● Embedded Security Device Support (Unterstützung eines Embedded Security-Geräts) ● Virtualization Technology (Virtualisierungstechnologie) ● Virtualization Technology Directed I/O (Virtualisierungstechnologie E/A geleitet) Embedded Security Device Support (Unterstützung eines Embedded Security-Geräts) (bestimmte Modelle) (Aktivieren/Deaktivieren) – Ermöglicht die Aktivierung und Deaktivierung des Embedded Security-Geräts. Zum Ändern dieser Einstellung muss der Computer ausgeschaltet und anschließend wieder eingeschaltet werden. **HINWEIS:** Zum Konfigurieren des Embedded Security-Geräts muss ein Setup-Kennwort festgelegt werden. ● Reset to Factory Settings (Auf Werkseinstellungen zurücksetzen) (bestimmte Modelle) (Nicht zurücksetzen/Zurücksetzen) – Beim Zurücksetzen auf die Werkseinstellungen werden alle Sicherheitsschlüssel gelöscht. Zum Ändern dieser Einstellung muss der Computer ausgeschaltet und anschließend wieder eingeschaltet werden. **ACHTUNG:** Das Embedded Security-Gerät ist eine wichtige Komponente vieler Sicherheitssysteme. Das Löschen der Sicherheitsschlüssel verhindert den Zugriff auf Daten, die durch das Embedded Security-Gerät geschützt werden. Wenn Sie die Option zum Zurücksetzen auf die Werkseinstellungen wählen, können viele Daten verloren gehen. ● Reset authentication credentials (Authentifizierungsdaten zurücksetzen) (bestimmte Modelle) (Nicht zurücksetzen/Zurücksetzen) – Wenn Sie die Option zum Zurücksetzen wählen, wird die Authentifizierung beim Einschalten deaktiviert und die Authentifizierungsdaten vom Embedded Security-Gerät gelöscht. Wenn Sie diese Einstellung ändern, muss der Computer ausgeschaltet und anschließend wieder eingeschaltet werden. OS Management of Embedded Security Device (Betriebssystemverwaltung des Embedded Security-Geräts) (bestimmte Modelle) (Aktivieren/Deaktivieren) – Mit dieser Option kann der Benutzer die Kontrolle des Betriebssystems über das Embedded Security-Gerät einschränken. Zum Ändern dieser Einstellung muss der Computer ausgeschaltet und anschließend wieder eingeschaltet werden. Mit dieser Option kann der Benutzer die Kontrolle des Betriebssystems über das Embedded Security-Gerät einschränken. ● Reset of Embedded Security Device through OS (Zurücksetzen des Embedded Security-Geräts durch das Betriebssystem) (bestimmte Modelle) (Aktivieren/Deaktivieren) – Mit dieser Option kann der Benutzer die Fähigkeit des Betriebssystems zum Anfordern einer Rücksetzung auf die Werkseinstellungen des Embedded Security-Geräts einschränken. Zum Ändern dieser Einstellung muss der Computer ausgeschaltet und anschließend wieder eingeschaltet werden. **HINWEIS:** Zum Aktivieren dieser Option muss ein Setup-Kennwort festgelegt werden. PAVP (bestimmte Modelle) (deaktiviert/min./max.) - PAVP aktiviert den geschützten Audio/Video-Pfad im Chipset. Hiermit kann geschützter High-Definition-Content angezeigt werden, dessen Wiedergabe andernfalls verboten ist. Bei der Auswahl von „Max.“ werden PAVP 96 MB Systemspeicher zugeordnet.

Kennwortschutz

Das Kennwort für den Systemstart verhindert eine unbefugte Verwendung des Computers, indem für den Zugriff auf Anwendungen oder Daten bei jedem Einschalten oder Neustart des Computers die Eingabe eines Kennworts verlangt wird. Das Setup-Kennwort verhindert insbesondere den unbefugten Zugriff auf Computer Setup und kann auch zur Übergehung des Kennworts für den Systemstart verwendet werden. Dabei wird auch dann der Zugriff auf den Computer gewährt, wenn bei der Eingabeaufforderung für das Systemstart-Kennwort statt dessen das Setup-Kennwort eingegeben wird.

Dabei kann ein Kennwort für das gesamte Netzwerk festgelegt werden, so dass der Systemadministrator sich für Wartungsarbeiten bei allen Netzwerksystemen anmelden kann, ohne das betreffende Kennwort für den Systemstart zu kennen.

HINWEIS: System Software Manager (SSM) kann verwendet werden, um über das Betriebssystem Microsoft Windows BIOS-Kennwörter zu erstellen oder zu verwalten. Weitere Informationen finden Sie im SSM-Benutzerhandbuch unter http://www.hp.com/go/ssm.

HINWEIS: HP Client Management Interface (HP CMI) bietet über das Betriebssystem Windows Zugriff auf die BIOS-Einstellungsverwaltung und auch auf BIOS-Kennwörter. Weitere Informationen finden Sie im technischen Whitepaper zu HP Client Management Interface unter http://www.hp.com/go/hpcmi.

Einrichten eines Setup-Kennworts über Computer Setup

Ist das System mit einem Embedded Security-Gerät ausgestattet, finden Sie weitere Informationen im *HP ProtectTools Security Manager-Handbuch* unter http://www.hp.com.) Die Einrichtung eines Setup-Kennworts über Computer Setup verhindert die Rekonfiguration des Computers (Verwendung des Dienstprogramms Computer Setup (f10)), solange kein Kennwort eingegeben wurde.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Neu starten**.
2. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, bevor das Betriebssystem startet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und vor dem Start des Betriebssystems erneut F10 drücken, damit das Dienstprogramm geöffnet wird.

3. Wählen Sie **Sicherheit** und anschließend **Setup-Kennwort**. Folgen Sie dann den Anleitungen auf dem Bildschirm.
4. Bevor Sie das Menü verlassen, klicken Sie auf **Datei** > **Änderungen speichern und beenden**.

Einrichten eines Kennworts beim Systemstart über Computer Setup

Die Einrichtung eines Kennworts für den Systemstart über Computer Setup verhindert den unbefugten Zugriff auf den Computer, wenn kein Kennwort eingegeben wird. Wenn ein Kennwort für den Systemstart festgelegt wurde, zeigt Computer Setup im Sicherheitsmenü eine Reihe von Kennwortoptionen an. Als Kennwortoptionen steht u. a. **Password Prompt on Warm Boot**

(Aufforderung zur Eingabe des Kennworts beim Warmstart) zur Auswahl. Bei Aktivierung dieser Option muss das Kennwort auch bei jedem Neustart eingegeben werden.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Neu starten**.
2. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, bevor das Betriebssystem startet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und vor dem Start des Betriebssystems erneut F10 drücken, damit das Dienstprogramm geöffnet wird.

3. Wählen Sie **Sicherheit** und anschließend **Kennwort für den Systemstart**. Folgen Sie dann den Anleitungen auf dem Bildschirm.
4. Bevor Sie das Menü verlassen, klicken Sie auf **File** (Datei) > **Save Changes and Exit** (Änderungen speichern und schließen).

Eingeben eines Kennworts für den Systemstart

Führen Sie die folgenden Schritte durch, um ein Kennwort für den Systemstart einzugeben:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Ausschalten** > **Neu starten**.
2. Wenn das Schlüsselsymbol auf dem Bildschirm angezeigt wird, geben Sie das aktuelle Kennwort ein und drücken dann die Eingabetaste.

   HINWEIS: Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

Wenn Sie das Kennwort falsch eingeben, erscheint ein durchgestrichenes Schlüsselsymbol. Versuchen Sie es noch einmal. Nach drei misslungenen Versuchen müssen Sie den Computer aus- und wieder einschalten, um fortfahren zu können.

Eingeben eines Setup-Kennworts

Ist das System mit einem Embedded Security-Gerät ausgestattet, finden Sie weitere Informationen im *HP ProtectTools Security Manager-Handbuch* unter http://www.hp.com.)

Wenn für den Computer ein Setup-Kennwort eingerichtet wurde, werden Sie jedes Mal zur Eingabe dieses Kennworts aufgefordert, wenn Sie das Programm Computer Setup starten.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Neu starten**.
2. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, bevor das Betriebssystem startet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und vor dem Start des Betriebssystems erneut F10 drücken, damit das Dienstprogramm geöffnet wird.

3. Wenn das Schlüsselsymbol auf dem Bildschirm angezeigt wird, geben Sie das Setup-Kennwort ein, und drücken Sie die Eingabetaste.

HINWEIS: Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

Wenn Sie das Kennwort falsch eingeben, erscheint ein durchgestrichenes Schlüsselsymbol. Versuchen Sie es noch einmal. Nach drei misslungenen Versuchen müssen Sie den Computer aus- und wieder einschalten, um fortfahren zu können.

Ändern des Kennworts für den Systemstart oder des Setup-Kennworts

Ist das System mit einem Embedded Security-Gerät ausgestattet, finden Sie weitere Informationen im *HP ProtectTools Security Manager-Handbuch* unter http://www.hp.com.)

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Ausschalten** > **Neu starten**.
2. Zum Ändern des Systemstart-Kennworts fahren Sie mit Schritt 3 fort.

   Um Computer Setup zu starten und das Setup-Kennwort zu ändern, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, bevor das Betriebssystem startet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und vor dem Start des Betriebssystems erneut F10 drücken, damit das Dienstprogramm geöffnet wird.

3. Wenn das Schlüsselsymbol angezeigt wird, geben Sie das aktuelle Kennwort, einen Schrägstrich(/) oder ein anderes Begrenzungszeichen, das neue Kennwort, einen weiteren Schrägstrich(/) bzw. ein anderes Begrenzungszeichen und ein zweites Mal das neue Kennwort ein, so dass der Eintrag wie folgt aussieht: `aktuelles Kennwort/neues Kennwort/neues Kennwort`

   HINWEIS: Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

4. Drücken Sie die Eingabetaste.

Das neue Kennwort gilt ab dem nächsten Start des Computers.

HINWEIS: Weitere Informationen zu Begrenzungszeichen finden Sie unter „Begrenzungszeichen auf landesspezifischen Tastaturen“ auf Seite 32. Das Kennwort für den Systemstart und das Setup-Kennwort können auch unter Verwendung der Sicherheitsfunktionen in Computer Setup geändert werden.

Löschen des Kennworts für den Systemstart oder des Setup-Kennworts

Ist das System mit einem Embedded Security-Gerät ausgestattet, finden Sie weitere Informationen im *HP ProtectTools Security Manager-Handbuch* unter http://www.hp.com.)

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Ausschalten** > **Neu starten**.
2. Zum Löschen des Systemstart-Kennworts fahren Sie mit Schritt 3 fort.

   Um Computer Setup zu starten und das Setup-Kennwort zu löschen, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, bevor das Betriebssystem startet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und vor dem Start des Betriebssystems erneut F10 drücken, damit das Dienstprogramm geöffnet wird.

3. Wenn das Schlüsselsymbol angezeigt wird, geben Sie das aktuelle Kennwort und einen Schrägstrich (/) oder ein anderes Begrenzungszeichen ein (siehe unten): `aktuelles Kennwort/`
4. Drücken Sie die Eingabetaste.

   HINWEIS: Weitere Informationen zu Begrenzungszeichen finden Sie unter „Begrenzungszeichen auf landesspezifischen Tastaturen“ auf Seite 32. Das Kennwort für den Systemstart und das Setup-Kennwort können auch unter Verwendung der Sicherheitsfunktionen in Computer Setup geändert werden.

Begrenzungszeichen auf landesspezifischen Tastaturen

Jede Tastatur wurde an die landesspezifischen sprachlichen Besonderheiten angepasst. Die Syntax und die Tasten, die Sie zum Ändern oder Löschen des Kennworts verwenden, sind abhängig von der Anordnung der Tasten auf Ihrer Tastatur.

Begrenzungszeichen auf landesspezifischen Tastaturen

/	Arabisch	-	Griechisch	/	Russisch
=	Belgisch	.	Hebräisch	-	Slowakisch
-	BHKMSS*	-	Ungarisch	-	Spanisch
/	Brasilianisch	-	Italienisch	/	Schwedisch/Finnisch
/	Chinesisch	/	Japanisch	-	Schweizerisch
-	Tschechisch	/	Koreanisch	/	Taiwanesisch
-	Dänisch	-	Lateinamerikanisch (Spanisch/ Portugiesisch)	/	Thailändisch
!	Französisch	-	Norwegisch	.	Türkisch
é	Kan. Französisch	-	Polnisch	/	Amerikanisches Englisch
-	Deutsch	-	Portugiesisch		

* Für Bosnien-Herzegowina, Kroatien, Montenegro, Serbien und Slowenien

Löschen von Kennwörtern

Wenn Sie Ihr Benutzerkennwort vergessen haben, können Sie nicht mehr auf Ihren Computer zugreifen. Eine Anleitung zum Löschen von Kennwörtern finden Sie im *Fehlerbeseitigungs-Handbuch*.

Ist das System mit einem Embedded Security-Gerät ausgestattet, finden Sie weitere Informationen im *HP ProtectTools Security Manager-Handbuch* unter http://www.hp.com.)

DriveLock

DriveLock ist eine Sicherheitsfunktion nach Branchenstandard, die den unbefugten Zugriff auf die Daten von ATA-Festplatten verhindert. DriveLock wurde als Erweiterung von Computer Setup entwickelt. Die Funktion steht nur für Laufwerke zur Verfügung, die den ATA-Befehlssatz für die Systemsicherheit unterstützen. DriveLock richtet sich an HP Kunden, deren oberste Priorität der Schutz der Daten ist. Für diese Kunden stehen die Kosten einer Festplatte und der Verlust der darauf gespeicherten Daten in keinem Verhältnis zu dem Schaden, der durch den unberechtigten Zugriff auf ihren Inhalt entstehen kann. Damit dieses hohe Sicherheitsniveau im Falle eines vergessenen Kennworts keine allzu großen Probleme verursacht, verwendet die HP Implementierung von DriveLock ein Sicherheitssystem mit zwei Kennwörtern. Dabei sollte ein Kennwort vom Systemadministrator festgelegt und verwendet werden, während das zweite normalerweise vom Benutzer erstellt und verwendet wird. Wenn beide Kennwörter vergessen werden, gibt es keine Möglichkeit mehr, die Laufwerksperre aufzuheben. Deshalb ist die Verwendung von DriveLock am sichersten, wenn die auf der Festplatte enthaltenen Daten in ein Firmeninformationssystem repliziert oder regelmäßig gesichert werden. Für den Fall, dass beide DriveLock-Kennwörter vergessen werden, bleibt der Zugriff auf die Festplatte für immer gesperrt. Dies stellt für Benutzer, die nicht dem obigen Kundenprofil entsprechen, unter Umständen ein inakzeptables Risiko dar. Für Benutzer, die diesem Profil entsprechen, ist dieses Risiko angesichts der auf der Festplatte gespeicherten Daten jedoch absolut akzeptabel.

Verwenden von DriveLock

Wenn eines oder mehrere Laufwerke den ATA-Befehlssatz für die Systemsicherheit unterstützen, wird im Sicherheitsmenü von Computer Setup die DriveLock-Option angezeigt. Der Benutzer kann wählen, ob er das Master-Kennwort festlegen oder DriveLock aktivieren möchte. Zur Aktivierung von DriveLock muss ein Benutzerkennwort eingegeben werden. Da die erste Konfiguration von DriveLock normalerweise vom Systemadministrator ausgeführt wird, sollte zuerst ein Masterkennwort festgelegt werden. HP empfiehlt die Festlegung eines Masterkennworts durch den Administrator, unabhängig davon, ob DriveLock aktiviert werden soll oder nicht. Dadurch hat der Administrator die Möglichkeit, DriveLock-Einstellungen zu ändern, wenn das Laufwerk einmal gesperrt sein sollte. Nachdem das Masterkennwort festgelegt wurde, kann der Administrator DriveLock aktivieren oder es deaktiviert lassen.

Im Fall einer gesperrten Festplatte fragt POST ein Kennwort zur Entsperrung ab. Wenn ein Kennwort für den Systemstart festgelegt wurde, das dem Benutzerkennwort des Geräts entspricht, fordert POST den Benutzer nicht zur erneuten Eingabe des Kennworts auf. Andernfalls wird der Benutzer zur Eingabe eines DriveLock-Kennworts aufgefordert. Bei einem Kaltstart kann entweder das Master- oder das Benutzerkennwort verwendet werden. Bei einem Warmstart muss dasselbe Kennwort eingegeben werden, mit dem das Laufwerk beim vorhergegangenen Kaltstart entsperrt wurde. Dabei haben die Benutzer zwei Versuche zur Kennworteingabe. Wenn bei einem Kaltstart zweimal das falsche Kennwort eingegeben wurde, wird POST zwar fortgesetzt, es besteht aber weiterhin kein Zugriff auf die Festplatte. Wenn der Benutzer bei einem Warmstart oder einem Neustart von Windows zweimal das falsche Kennwort eingegeben hat, wird POST angehalten, und der Benutzer wird aufgefordert, das System aus- und wieder einzuschalten.

DriveLock-Anwendungen

Den größten Nutzen entfaltet die DriveLock-Sicherheitsfunktion in einer Unternehmensumgebung. Dort hat der Systemadministrator die Aufgabe, die Festplatte zu konfigurieren und damit u. a. auch das DriveLock-Masterkennwort sowie ein temporäres Benutzerkennwort einzurichten. Falls ein Benutzer das Benutzerkennwort vergisst oder das Gerät an einen anderen Mitarbeiter weitergegeben wird, kann das Masterkennwort dazu verwendet werden, das Benutzerkennwort zurückzusetzen oder auf die Festplatte zuzugreifen.

HP empfiehlt Systemadministratoren, die DriveLock aktivieren möchten, die Erstellung einer Firmenrichtlinie zur Einrichtung und Verwaltung von Masterkennwörtern. Dadurch soll vermieden werden, dass ein Mitarbeiter vor seinem Ausscheiden aus der Firma absichtlich oder unabsichtlich beide DriveLock-Kennwörter festlegt. In einem solchen Fall würde die Festplatte unbrauchbar und müsste ersetzt werden. Außerdem könnte es passieren, dass Systemadministratoren, die kein Masterkennwort festlegen, selbst eine gesperrte Festplatte vorfinden und dadurch keine Routineüberprüfungen auf nicht autorisierte Software, andere Bestandskontrollfunktionen und Supportaktivitäten mehr ausführen können.

Benutzern mit niedrigeren Sicherheitsanforderungen empfiehlt HP die Aktivierung von DriveLock nicht. Dazu zählen private Benutzer oder Benutzer, die auf ihrer Festplatte im Normalfall keine streng geheimen Daten aufbewahren. Für diese Benutzer ist der mögliche Verlust einer Festplatte aufgrund von zwei vergessenen Kennwörtern größer als der Wert, der mit DriveLock geschützt werden soll. Der Zugriff auf Computer Setup und DriveLock kann durch das Setup-Kennwort eingeschränkt werden. Durch das Festlegen eines Setup-Kennworts, das nicht an Endbenutzer weitergegeben wird, können Systemadministratoren vermeiden, dass Benutzer DriveLock aktivieren.

Smart Cover Sensor

Cover Removal Sensor (bestimmte Modelle) ist eine Kombination aus Hardware- und Softwaretechnologie, die entsprechende Meldungen ausgibt, wenn die Gehäuseabdeckung oder das Seitenteil des Computers abgenommen wurden. Es gibt drei Sicherheitsstufen, die in der nachstehenden Tabelle beschrieben werden.

Tabelle 11-2 Smart Cover Sensor – Schutzstufen

Stufe	Einstellung	Beschreibung
Stufe 0	Disabled (Deaktiviert)	Der Smart Cover Sensor ist deaktiviert (Standardeinstellung).
Stufe 1	Notify User (Benutzer benachrichtigen)	Wenn der Computer neu gestartet wird, wird gemeldet, dass die Gehäuseabdeckung bzw. die Seitenabdeckungen entfernt wurden.
Stufe 2	Setup-Kennwort	Wenn der Computer neu gestartet wird, wird gemeldet, dass die Gehäuseabdeckung bzw. die Seitenabdeckungen entfernt wurden. Sie müssen das Setup-Kennwort eingeben, um fortfahren zu können.

HINWEIS: Diese Einstellungen können mit Hilfe von Computer Setup geändert werden. Weitere Informationen zu Computer Setup finden Sie im *Computer Setup (f10) Utility-Handbuch*.

Einstellen der Schutzstufe für den Smart Cover Sensor

So legen Sie die Schutzstufe für den Smart Cover Sensor fest:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Neu starten**.
2. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, bevor das Betriebssystem startet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und vor dem Start des Betriebssystems erneut F10 drücken, damit das Dienstprogramm geöffnet wird.

3. Wählen Sie **Sicherheit** > **Smart Cover** > **Cover Removal Sensor**, und aktivieren Sie dann die gewünschte Schutzstufe.
4. Bevor Sie das Menü verlassen, klicken Sie auf **Datei** > **Änderungen speichern und beenden**.

Smart Cover Lock

Das Smart Cover Lock ist eine softwaregesteuerte Gehäusesperre, mit der eine Reihe von HP Computern ausgestattet sind. Sie verhindert den unbefugten Zugriff auf die internen Komponenten des Computers. Die Computer werden mit deaktiviertem Smart Cover Lock geliefert.

ACHTUNG: Für den maximalen Schutz der Gehäusesperre müssen Sie ein Setup-Kennwort einrichten. Das Setup-Kennwort verhindert den unbefugten Zugriff auf das Dienstprogramm „Computer Setup“.

HINWEIS: Das Smart Cover Lock ist als Zusatzoption für bestimmte Systeme erhältlich.

Sperren des Smart Cover Lock

So aktivieren (sperren) Sie das Smart Cover Lock:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Neu starten**.
2. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, bevor das Betriebssystem startet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und vor dem Start des Betriebssystems erneut F10 drücken, damit das Dienstprogramm geöffnet wird.

3. Wählen Sie **Sicherheit** > **Smart Cover** > **Cover Lock** (Gehäusesperre) > **Lock option** (Sperroption).
4. Bevor Sie das Menü verlassen, klicken Sie auf **Datei** > **Änderungen speichern und beenden**.

Aufheben der Sperre des Smart Cover Lock

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start** > **Herunterfahren** > **Neu starten**.
2. Um Computer Setup zu starten, drücken Sie sofort nach dem Einschalten des Computers die Taste F10, bevor das Betriebssystem startet. Drücken Sie die Eingabetaste, um ggf. den Titelbildschirm zu überspringen.

   HINWEIS: Wenn Sie F10 nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer neu starten und vor dem Start des Betriebssystems erneut F10 drücken, damit das Dienstprogramm geöffnet wird.

3. Wählen Sie **Sicherheit** > **Smart Cover** > **Cover Lock** (Gehäusesperre) > **Unlock** (Entsperren).
4. Bevor Sie das Menü verlassen, klicken Sie auf **Datei** > **Änderungen speichern und beenden**.

Verwenden des Smart Cover-FailSafe-Schlüssels

Wenn das Smart Cover Lock aktiviert ist und Sie das Benutzerkennwort nicht eingeben können, um die Sperre zu deaktivieren, brauchen Sie einen Smart Cover FailSafe-Schlüssel, um die Gehäuseabdeckung öffnen zu können. Sie brauchen den Schlüssel in den folgenden Fällen:

- Stromausfall
- Fehlgeschlagener Systemstart
- Ausfall einer PC-Komponente (z. B. Prozessor oder Netzteil)
- Vergessenes Kennwort

ACHTUNG: Der Smart Cover-FailSafe-Schlüssel ist ein spezielles bei HP erhältliches Tool. Seien Sie vorbereitet. Bestellen Sie diesen Schlüssel bei einem Servicepartner, bevor Sie ihn benötigen.

Führen Sie eines der folgenden Verfahren durch, um den FailSafe-Schlüssel zu erhalten:

- Wenden Sie sich an einen HP Servicepartner.
- Rufen Sie die in der Garantieerklärung genannte Rufnummer an.

Weitere Informationen zur Verwendung des Smart Cover FailSafe-Schlüssels finden Sie im *Hardware-Referenzhandbuch*.

Kabel-Diebstahlsicherung

Sie können an der Anschlussleiste auf der Rückseite des Computers (bestimmte Modelle) eine Kabel-Diebstahlsicherung anbringen und damit den Computer an einen fest installierten Gegenstand anschließen.

Eine Anleitung mit den entsprechenden Abbildungen finden Sie im *Hardware-Referenzhandbuch*.

Fingerprint Identification Technology

Die HP Fingerprint Identification Technology macht die Eingabe eines Benutzerkennworts überflüssig, erhöht die Netzwerksicherheit, vereinfacht den Anmeldungsvorgang und verringert die mit dem Management von Firmennetzwerken verbundenen Kosten. Wegen ihres erschwinglichen Preises ist sie nicht mehr nur High-Tech-Organisationen mit hohem Sicherheitsbedürfnis vorbehalten.

HINWEIS: Die Unterstützung für die Fingerprint Identification Technology hängt von dem jeweiligen Modell ab.

Fehlerbenachrichtigung und Wiederherstellung

Durch die Kombination von innovativer Hardware- und Softwaretechnologie sorgen die Funktionen zur Fehlermeldung und Fehlerbehebung dafür, dass der Datenverlust und Ausfallzeiten vermieden werden.

Wenn der Computer an ein Netzwerk angeschlossen ist, das von HP Client Manager überwacht wird, sendet er eine Fehlermeldung an die Netzwerk-Management-Anwendung. HP Client Manager Software ermöglicht aber auch die Remote-Einplanung von Diagnosetests, so dass diese automatisch auf allen verwalteten PCs ausgeführt und eventuell festgestellte Fehler in einem Bericht protokolliert werden.

Drive Protection System

Das Drive Protection System (DPS) ist ein Diagnose-Tool, mit dem die Festplatten bestimmter HP Computer ab Werk ausgestattet sind. Das Programm soll die Diagnose von Problemen ermöglichen, die andernfalls zu einem unnötigen Festplattenaustausch führen könnten.

Jede Festplatte wird vor dem Einbau in einen HP Computer mittels DPS getestet. Dabei werden wichtige Informationen auf der Festplatte gespeichert. Die Testergebnisse werden bei jeder Ausführung von DPS auf der Festplatte gespeichert. Diese Informationen erleichtern dem Servicepartner eine Diagnose der Bedingungen, aufgrund derer Sie DPS ausgeführt haben. Eine Anleitung zur Verwendung von DPS finden Sie im *Fehlerbeseitigungs-Handbuch*.

Überspannungsschutz

Durch ein integriertes überspannungstolerantes Netzteil wird eine größere Zuverlässigkeit erzielt, wenn der Computer Spannungsspitzen ausgesetzt wird. Dieses Netzteil ist so ausgelegt, dass eine Überspannung von bis zu 2.000 V ohne Systemausfall oder Datenverluste neutralisiert werden kann.

Thermosensor

Der Temperatursensor ist eine Hardware- und Softwarefunktion zur internen Überwachung der Temperatur des Computers. Diese Funktion zeigt eine Warnmeldung an, wenn der normale Bereich überschritten wird. Dies gibt Ihnen Zeit, entsprechende Maßnahmen zu ergreifen, bevor interne Komponenten beschädigt werden oder Daten verloren gehen.

△ **ACHTUNG:** Bei einer hohen Temperatur besteht die Gefahr von Systembeschädigung oder Datenverlust.

Index