



Desktop Management

Business Desktops

Dokument-Teilenummer: 312947-041

März 2003

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

© 2002 Hewlett-Packard Company
© 2002 Hewlett-Packard Development Company, L.P.

HP, Hewlett-Packard und das Hewlett-Packard Logo sind Marken der Hewlett-Packard Company in den USA und anderen Ländern.

Compaq und das Compaq Logo sind Marken der Hewlett-Packard Development Company, L.P. in den USA und anderen Ländern.

Microsoft, MS-DOS, Windows und Windows NT sind Marken der Microsoft Corporation in den USA und anderen Ländern.

Alle anderen in diesem Handbuch verwendeten Produktnamen sind unter Umständen Marken der jeweiligen Unternehmen.

Die Hewlett-Packard Company haftet nicht für technische oder redaktionelle Fehler und Mängel in diesem Dokument. Ferner übernimmt die Hewlett-Packard Company keine Haftung für Schäden, die direkt oder indirekt auf die Bereitstellung, Leistung und Nutzung dieses Materials zurückzuführen sind. Die Informationen in diesem Dokument werden ohne Gewähr für ihre Richtigkeit zur Verfügung gestellt und können ohne vorherige Ankündigung geändert werden. Darüber hinaus werden keine Gewährleistungen übernommen, einschließlich der ausdrücklichen bzw. konkludenten Gewährleistungen für die Tauglichkeit und Eignung für einen bestimmten Zweck. Die Garantien für HP Produkte werden ausschließlich in der entsprechenden, zum Produkt gehörigen Garantieerklärung beschrieben. Aus dem vorliegenden Dokument sind keine weiter reichenden Garantieansprüche abzuleiten.

Dieses Dokument enthält Informationen, die durch das Urheberrecht geschützt sind. Ohne schriftliche Genehmigung der Hewlett-Packard Company darf dieses Dokument weder kopiert noch in anderer Form vervielfältigt oder übersetzt werden.



VORSICHT: In dieser Form hervorgehobener Text weist darauf hin, dass die Nichtbeachtung zu Verletzungen oder zum Tod führen kann.



ACHTUNG: In dieser Form hervorgehobener Text weist darauf hin, dass die Nichtbeachtung zu Beschädigungen der Geräte oder zum Verlust von Daten führen kann.

Desktop Management

Business Desktops

Erste Ausgabe (März 2003)

Dokument-Teilenummer: 312947-041

Desktop Management

Erste Konfiguration und erster Einsatz	2
Remote System Installation	3
Software-Aktualisierung und -Management	4
Altiris eXpress	4
Altiris eXpress PC Transplant Pro	6
HP Client Manager Software	6
System Software Manager	7
HP Proactive Notification (HPPN)	7
ActiveUpdate	8
ROM-Flash	8
Remote ROM Flash	9
FailSafe Boot Block ROM	9
Replizieren des Setup	12
Dual-State-Netzschalter	13
Power Management	14
WWW-Site	15
Bausteine und Partner	15
Bestandsüberwachung und Sicherheit	16
Kennwort-Schutz	20
Einrichten eines Setup-Kennworts über Computer Setup	20
Einrichten eines Kennworts beim Systemstart über Computer Setup	21
DriveLock	25
Smart Cover Sensor	28
Smart Cover Lock	29
Master Boot Record Security (Master Boot Record-Sicherheit)	32
Maßnahmen vor der Partitionierung oder Formatierung der aktuellen bootfähigen Festplatte	34
Kabelschloss	35
Fingerprint Identification Technology	35

Fehlermeldung und Fehlerbehebung	36
Drive Protection System	36
Überspannungsschutz	37
Thermosensor	37

Index

Desktop Management

HP Intelligent Manageability bietet standardbasierte Lösungen zur Verwaltung und Steuerung von Desktops, Workstations und Notebook-PCs in einer Netzwerkkumgebung. 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 steht HP an der Spitze eines branchenweiten Bemühens, die für den effektiven Einsatz sowie die Konfiguration und Verwaltung von Desktops, Workstations und Notebook-PCs erforderlichen Standards und Infrastrukturen zu entwickeln. HP arbeitet eng mit marktführenden Anbietern von Management-Software-Lösungen zusammen, um die Kompatibilität zwischen Intelligent Manageability und diesen Produkten sicherzustellen. Intelligent Manageability ist ein wichtiger Aspekt des umfassenden Engagements von HP, Ihnen PC Lifecycle-Lösungen für alle vier Phasen des Lebenszyklus eines Desktop-PCs anzubieten – von der Planung und dem Einsatz über die Verwaltung bis zur Umstellung.

Dieses Handbuch fasst die Möglichkeiten und Funktionen der sieben Hauptkomponenten des Desktop Management zusammen.

- Erste Konfiguration und erster Einsatz
- Remote System Installation
- Software-Aktualisierung und -Management
- ROM-Flash
- Bausteine und Partner
- Bestandsüberwachung und Sicherheit
- Fehlermeldung und Fehlerbeseitigung



Die Unterstützung spezieller, in diesem Handbuch beschriebener Funktionen kann sich je nach Modell oder Software-Version unterscheiden.

Erste Konfiguration und erster Einsatz

Die Computer werden mit vorinstalliertem Systemsoftware-Image geliefert. Nach einem kurzen Vorgang des „Auspackens“ der Software 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-Einsatz-Tools, wie etwa Altiris eXpress, 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. Der Abschnitt zum PC-Einsatz auf der Website zu Lösungen und Dienstleistungen (<http://www.compaq.com/solutions/pcsolutions>) bietet Ihnen Informationen zur Auswahl des besten Verfahrens.

Die *Restore Plus* CD, das ROM-basierte Setup und die Hardware mit ACPI-Unterstützung bieten zusätzliche Hilfe bei der Wiederherstellung der Systemsoftware, dem Konfigurations-Management, der Fehlerbeseitigung sowie bei der Energieverwaltung.

Remote System Installation

Remote System Installation erlaubt Ihnen, Ihr System mit Hilfe der Software und der Konfigurationsinformationen von einem Netzwerk-Server zu starten und zu installieren. Hierfür wird das Preboot Execution Environment (PXE) gestartet. Die Remote-Installationsfunktion wird normalerweise als Tool zur Systemeinrichtung und -konfiguration verwendet und kann darüber hinaus für die folgenden Aufgaben eingesetzt werden:

- Formatieren einer Festplatte
- Einsetzen eines Software-Images auf einem oder mehreren neuen PCs
- Installieren von Anwendungssoftware oder Treibern
- Aktualisieren des Betriebssystems, der Anwendungssoftware oder der Treiber

Drücken Sie die Taste **F12**, um Remote System Installation zu starten, wenn die Meldung **F12 = Network Service Boot** (Starten über Netzwerk) in der unteren rechten Ecke der HP Logoanzeige erscheint. Folgen Sie den Anleitungen auf dem Bildschirm, um fortzufahren.

HP und Altiris, Inc. stellen gemeinsam Tools zur Verfügung, die den Einsatz und das Management von Firmen-PCs vereinfachen, weniger zeitaufwendig gestalten, die Total Cost of Ownership senken und die HP PCs zu den Client-PCs mit der besten Manageability in Unternehmen machen.

Software-Aktualisierung und -Management

HP bietet verschiedene Tools für Software-Aktualisierung und -Management auf Desktop-Computern und Workstations: Altiris eXpress; Altiris eXpress PC Transplant Pro; HP Client Manager Software, eine Altiris eXpress Lösung; System Software Manager; HP Proactive Notification und ActiveUpdate.

Altiris eXpress

Dank einer noch engeren Partnerschaft zwischen HP und Altiris können nun branchenführende Lösungen angeboten werden, die die Verwaltung der Hardware und Software für Desktop-Computer, Notebooks, Handheld-Geräte und Server während des gesamten Lebenszyklus dieser Geräte vereinfachen. Altiris eXpress ermöglicht dem Systemadministrator die Erstellung und den schnellen Einsatz eines nach dem Firmenstandard angepassten Software-Images auf einem oder mehreren vernetzten Client-PCs mit einer Schnittstelle, die so einfach zu verwenden ist wie der Windows Explorer. Altiris eXpress unterstützt Preboot Execution Environment (PXE). Bei Verwendung der Funktionen von Altiris eXpress und Remote System Installation auf dem HP Computer ist es für den Systemadministrator nicht erforderlich, das Software-Image auf jedem neuen PC einzeln zu implementieren.

Die Altiris eXpress Lösungen bieten eine effiziente und effektive Methode, bestehende Prozesse zu automatisieren und Problembereiche in der IT-Umgebung anzugehen. Die Web-basierte Infrastruktur von Altiris eXpress verschafft Ihnen die Flexibilität, Ihre Systeme zu jeder Zeit und von jedem Ort aus zu verwalten – sogar von Ihrem iPAQ Pocket PC aus!

Die Altiris eXpress Lösungen sind modular und erweiterbar, so dass sowohl die Anforderungen von Arbeitsgruppen als auch die des gesamten Unternehmens erfüllt werden. Diese Lösungen können in Client-Management-Tools anderer Anbieter integriert werden und bieten Erweiterungen für Microsoft BackOffice/SMS.

Die erweiterten Altiris eXpress Lösungen konzentrieren sich auf vier zentrale IT-Bereiche:

- Einsatz und Migration
- Software und Operations Management
- Bestandsverwaltung
- Help Desk und Problemlösung

Nach wenigen Minuten der Installation können Sie mit Altiris eXpress ein Festplatten-Image mit dem Betriebssystem, der Anwendungssoftware und dem Altiris eXpress Client installieren, ohne dass eine separate Startdiskette verwendet werden muss. Mit Altiris eXpress können Netzwerkadministratoren folgende Aufgaben durchführen:

- Erstellen eines neuen oder Bearbeiten eines bereits vorhandenen Images oder Cloning eines PCs mit idealem Image im Netzwerk.
- Erstellen einer beliebigen Anzahl von benutzerdefinierten Festplatten-Images für eine Vielzahl von Arbeitsgruppen.
- Bearbeiten vorhandener Image-Dateien statt der Erstellung vollkommen neuer Dateien. Dies ist möglich, da mit Altiris eXpress die Dateien in ihrem ursprünglichen Format gespeichert werden, also als NTFS-, FAT16- oder FAT32-Dateien.
- Einrichten eines Ereignisses für neue PCs – eines Skripts, das automatisch ausgeführt wird, wenn ein neuer PC dem Netzwerk hinzugefügt wird. Mit dem Skript kann beispielsweise die Festplatte eines PCs formatiert, ein Flash des ROM-BIOS durchgeführt und ein vollständiges Standardsoftware-Image installiert werden.
- Festlegen des Zeitplans für ein Ereignis, das für eine Gruppe von Computern ausgeführt werden soll.

Altiris eXpress bietet auch benutzerfreundliche Software-Verteilungsmöglichkeiten. Altiris eXpress kann zur Aktualisierung von Betriebssystemen und Anwendungssoftware von einer zentralen Konsole aus verwendet werden. Wenn Altiris eXpress in Verbindung mit System Software Manager oder HP Client Manager verwendet wird, können auch ROM-BIOS und Gerätetreiber aktualisiert werden.

Weitere Informationen finden Sie unter <http://www.compaq.com/easydeploy>.

Altiris eXpress PC Transplant Pro

Altiris eXpress PC Transplant Pro ermöglicht eine problemlose PC-Migration, indem alte Einstellungen, Voreinstellungen und Daten erhalten bleiben und auf schnelle und einfache Weise in die neue Umgebung überstellt werden. Anstelle von Stunden oder sogar Tagen dauert dieser Vorgang nur wenige Minuten, und schon können Sie mit Ihrem Desktop-Computer in gewohnter Weise arbeiten.

Weitere Informationen und Einzelheiten zum Herunterladen einer voll funktionsfähigen 30-Tage-Testversion finden Sie unter <http://www.compaq.com/easydeploy>.

HP Client Manager Software

HP Client Manager Software (HP CMS) integriert die HP Intelligent Manageability-Technologie innerhalb von Altiris eXpress und bietet so erstklassige Hardware-Management-Funktionen für HP Zugangsgeräte, wie z. B.:

- Ausführliche Ansichten des Hardware-Inventars für die Bestandsverwaltung
- Überwachung des PC-Zustands und Diagnose
- Proaktive Benachrichtigung über Änderungen in der Hardware-Umgebung
- Über das Web zugängliche Berichtserstellung von wichtigen Detailinformationen, wie beispielsweise Warnmeldungen bei Geräteüberhitzung, mangelndem Speicherplatz usw.
- Remote-Aktualisierung von Systemsoftware, wie beispielsweise Gerätetreiber und ROM-BIOS

Weitere Informationen zu HP Client Manager finden Sie unter <http://www.compaq.com/easydeploy>.

System Software Manager

System Software Manager (SSM) ist ein Dienstprogramm, mit dem Software auf Systemebene auf mehreren Systemen gleichzeitig aktualisiert werden kann. Wenn SSM auf einem PC-Client-System ausgeführt wird, erkennt es sowohl Hardware- als auch Software- Versionen und aktualisiert die betreffende Software dann von einem zentralen Repository, dem so genannten Dateispeicher, aus. Treiberversionen, die von SSM unterstützt werden, sind auf der Website zum Herunterladen von Treibern sowie auf der Support Software CD durch ein spezielles Symbol gekennzeichnet. Besuchen Sie zum Herunterladen des Dienstprogramms oder zum Abrufen weiterer Informationen zu SSM die folgende Website: <http://www.compaq.com/im/ssmwp.html>.

HP Proactive Notification (HPPN)

HP Proactive Notification versendet auf Basis der Eintragungen auf der sicheren Website **Subscriber's Choice** proaktiv und 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 an den meisten Computern und Servern für Unternehmen informiert werden.
- Eine E-Mail mit Informationen, Ratschlägen und Hinweisen für Kunden, Sicherheitsmitteilungen und Treiber-Warmmeldungen für die meisten Computer und Server für Unternehmen.

Durch die Erstellung Ihres persönlichen Profils wird gewährleistet, dass Sie nur Informationen erhalten, die für Ihre IT-Umgebung von Interesse sind. Weitere Informationen zu HPPN und zur Erstellung Ihres benutzerdefinierten Profils finden Sie unter folgender Adresse: <http://www.hp.com/united-states/subscribe/>

ActiveUpdate

ActiveUpdate ist eine Client-basierte Anwendung von HP. Der ActiveUpdate Client wird auf Ihrem lokalen System ausgeführt und verwendet Ihr benutzerdefiniertes Profil, um Software-Aktualisierungen für die meisten Computer und Server für Unternehmen von HP proaktiv und automatisch herunterzuladen.

Weitere Informationen zu ActiveUpdate sowie zum Herunterladen der Anwendung und zum Erstellen eines benutzerdefinierten Profils finden Sie unter folgender Adresse:

<http://www.compaq.com/activeupdate>.

ROM-Flash

Ihr Computer verfügt über einen programmierbaren Flash-ROM-Speicher (ROM = Read Only Memory, Nur-Lese-Speicher). Wenn Sie ein Setup-Kennwort in Computer Setup (F10) Utility einrichten, können Sie verhindern, dass der ROM-Speicher unbeabsichtigt aktualisiert oder überschrieben wird. Dies ist wichtig zur Gewährleistung des fehlerfreien Betriebs des Computers. Wenn Sie den ROM-Speicher aktualisieren müssen oder möchten, können Sie wie folgt vorgehen:

- Bestellen Sie eine aktuelle *ROMPaq*TM Diskette von HP.
- Laden Sie die neuesten ROMPaq Images unter <http://www.hp.com/support> herunter.



ACHTUNG: Für den maximalen Schutz des ROM-Speichers müssen Sie ein Setup-Kennwort einrichten. Das Setup-Kennwort verhindert die unbefugte Aktualisierung des ROM-Speichers. Mithilfe von System Software Manager kann der Systemadministrator das Setup-Kennwort auf mehreren PCs gleichzeitig einstellen. Weitere Informationen finden Sie unter folgender Adresse:

<http://www.compaq.com/im/ssmwp.html>.

Remote ROM Flash

Remote ROM Flash ermöglicht dem Systemadministrator, den ROM-Speicher von HP Computern direkt von der zentralen Netzwerk-Management-Konsole aus auf sichere Art und Weise zu aktualisieren. Da der Systemadministrator diese Aufgabe für mehrere Computer und PCs remote durchführen kann, ergibt sich dadurch ein konsistenter Einsatz und eine bessere Überwachung von HP PC ROM-Images über das Netzwerk. Dies führt außerdem zu höherer Produktivität und niedrigeren Total Cost of Ownership.



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

Weitere Details zu Remote ROM Flash finden Sie in den Informationen zu HP Client Manager oder System Software Manager unter <http://www.compaq.com/easydeploy>.

FailSafe Boot Block ROM

FailSafe Boot Block ROM ermöglicht eine Wiederherstellung des Systems im unwahrscheinlichen Fall eines ROM-Flash-Fehlers, z. B. bei einem Stromausfall während einer ROM-Aktualisierung. Der Boot-Block ist ein flash-geschützter Bereich des ROM-Speichers, der jedes Mal die Gültigkeit des ROM-Flash-Speichers überprüft, wenn der Computer eingeschaltet wird.

- Wenn der ROM-Speicher des Systems gültig ist, startet das System normal.
- Wenn der ROM-Speicher den Gültigkeitstest nicht besteht, bietet FailSafe Boot Block ROM ausreichend Unterstützung, damit das System von einer ROMPaq Diskette aus starten kann, die dem ROM-Speicher ein gültiges Image zuweist.

Wenn im Boot-Block ein ungültiger System-ROM-Speicher festgestellt wird, leuchtet die ROTE Betriebs-LED achtmal im Abstand von jeweils einer Sekunde, mit einer zweisekündigen Pause. Gleichzeitig wird auch ein achtfacher Signalton ausgegeben. Eine Meldung wird angezeigt, die angibt, dass das System in den Boot-Block-Wiederherstellungsmodus schaltet (modellabhängig).


Wenn Sie das System wiederherstellen möchten, nachdem es in den Boot-Block-Wiederherstellungsmodus geschaltet hat, führen Sie folgende Schritte aus:

1. Wenn sich eine Diskette im Laufwerk befindet, nehmen Sie diese aus dem Laufwerk, und schalten Sie den Computer aus.
2. Legen Sie eine ROMPaq Diskette in das Diskettenlaufwerk ein.
3. Schalten Sie den Strom wieder ein.
4. Wenn keine ROMPaq Diskette gefunden wird, werden Sie aufgefordert, diese Diskette einzulegen und den Computer neu zu starten.
5. Wenn ein Setup-Kennwort eingerichtet wurde, leuchtet die LED-Anzeige der **Feststelltaste**, und Sie werden zur Eingabe des Kennworts aufgefordert.
6. Geben Sie das Setup-Kennwort ein.
7. Wenn das System erfolgreich von der Diskette startet und den ROM erfolgreich umprogrammiert, beginnen die drei LED-Anzeigen auf der Tastatur zu leuchten. Eine lauter werdende Abfolge von akustischen Signalen kennzeichnet zusätzlich den erfolgreichen Abschluss des Vorgangs.
8. Nehmen Sie die Diskette aus dem Laufwerk, und schalten Sie den Computer aus.
9. Starten Sie den Computer anschließend neu.

Die folgende Tabelle gibt einen Überblick über die von Boot Block ROM verwendeten verschiedenen Kombinationen der LED-Anzeigen auf der Tastatur (insofern eine PS/2-Tastatur angeschlossen ist) und ihre Bedeutungen sowie die Schritte in Verbindung mit diesen Kombinationen.

Von Boot Block ROM verwendete Kombinationen der LED-Anzeigen auf der Tastatur

LED	LED-Farbe	LED-Aktivität	Zustand/Meldung
Num	Grün	Ein	ROMPaq Diskette nicht vorhanden oder fehlerhaft oder Laufwerk nicht bereit.
Feststelltaste	Grün	Ein	Kennwort eingeben.
Num, Feststelltaste, Roller	Grün	Zweimal ein und aus (begleitet von einem langen und drei kurzen Tönen)	ROM-Flash-Fehler.
Num, Feststelltaste, Roller	Grün	Ein	Boot Block ROM-Flash erfolgreich. Schalten Sie den Computer aus und anschließend wieder ein, um neu zu starten.

 Auf USB-Tastaturen wird die Diagnosefunktion der Tastatur-LEDs nicht unterstützt.

Replizieren des Setup

Dieses Verfahren ermöglicht es dem Systemadministrator, ohne großen Aufwand eine Setup-Konfiguration auf andere Computer des gleichen Modells zu kopieren. Auf diese Weise kann die Konfiguration mehrerer Computer schneller und mit größerer Einheitlichkeit durchgeführt werden. So replizieren Sie das Setup:

1. Öffnen Sie das Menü von Computer Setup Utility (F10).
2. Klicken Sie auf **File > Save to Diskette** (Datei > Speichern auf Diskette). Folgen Sie den Anleitungen auf dem Bildschirm.



Für den Vorgang ist ein Diskettenlaufwerk oder ein unterstütztes USB-Flash-Media-Gerät wie DiskOnKey erforderlich.

3. Um die Konfiguration zu replizieren, klicken Sie auf **File > Restore from Diskette** (Datei > Wiederherstellen von Diskette), und folgen Sie den Anleitungen auf dem Bildschirm.

Altiris eXpress, System Software Manager und PC Transplant vereinfachen die Replikation der Konfiguration und benutzerdefinierten Einstellungen auf einem PC sowie das Kopieren dieser Daten auf einen oder mehrere andere PCs. Weitere Informationen finden Sie unter folgender Adresse: <http://www.compaq.com/easydeploy>.

Dual-State-Netzschalter

Bei aktivierter ACPI-Funktion (Advanced Configuration and Power Interface) für Windows 98, Windows 2000 und Windows XP übernimmt der Netzschalter entweder die Funktion des Ein-/Aus-Schalters oder der Standby-Taste. Im Standby-Modus wird die Stromzufuhr nicht komplett unterbrochen, sondern der Computer schaltet auf geringen Stromverbrauch um. Dadurch können Sie schnell in den Energiesparmodus schalten, ohne die Anwendungen schließen zu müssen, und Sie können ohne Datenverlust schnell in den gleichen Betriebszustand zurückkehren.

So ändern Sie die Konfiguration des Netzschalters:

1. Klicken Sie unter Windows 2000 mit der linken Maustaste auf die Schaltfläche **Start**, und wählen Sie **Einstellungen > Systemsteuerung > Energieoptionen**.

Klicken Sie unter Windows XP mit der linken Maustaste auf die Schaltfläche **Start**, und wählen Sie **Systemsteuerung > Leistung und Wartung > Energieoptionen**.

2. Öffnen Sie unter **Eigenschaften von Energieoptionen** die Registerkarte **Erweitert**.
3. Wählen Sie im Abschnitt für die Netzschaltervorgänge die gewünschten Einstellungen für den Netzschalter aus.

Wenn Sie den Netzschalter als Standby-Taste konfiguriert haben, wird das System durch Drücken des Schalters auf sehr geringen Stromverbrauch (Standby-Modus) umgeschaltet. Wenn Sie erneut auf die Standby-Taste drücken, 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.

Power Management

Power Management ist eine Energiesparfunktion, die einige Komponenten des Computers abschaltet, wenn diese nicht gebraucht werden. Hierdurch kann Energie gespart werden, ohne dass der Computer ausgeschaltet werden muss.

Wenn ACPI (Advanced Configuration and Power Interface) für Windows 98, Windows 2000, Windows Me und Windows XP aktiviert wurde, können über das Betriebssystem Timeout-Werte (zulässiger Zeitraum der Inaktivität, bevor die Komponenten heruntergefahren werden) aktiviert, angepasst oder deaktiviert werden.

1. Klicken Sie unter Windows 2000 mit der linken Maustaste auf die Schaltfläche **Start**, und wählen Sie **Einstellungen > Systemsteuerung > Energieoptionen**.

Klicken Sie unter Windows XP mit der linken Maustaste auf die Schaltfläche **Start**, und wählen Sie **Systemsteuerung > Leistung und Wartung > Energieoptionen**.

2. Öffnen Sie unter **Eigenschaften von Energieoptionen** die Registerkarte **Energieschemas**.
3. Wählen Sie die gewünschten Einstellungen für die Energieschemas aus.

Verwenden Sie die Option **Eigenschaften von Anzeige**, um die Energiespareinstellungen für den Monitor festzulegen, zu ändern oder zu deaktivieren. Um die Option **Eigenschaften von Anzeige** aufzurufen, klicken mit der rechten Maustaste auf den Windows Desktop, und wählen Sie **Eigenschaften**.

WWW-Site

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

Wenn Sie ein neues oder überarbeitetes Betriebssystem auf Ihrem Computer installieren, ist es wichtig, dass Sie auch die für das jeweilige Betriebssystem entwickelte Support-Software installieren. Wenn Sie mit einer Version von Microsoft Windows arbeiten möchten, die sich von der auf dem Computer vorinstallierten Version unterscheidet, müssen die entsprechenden Gerätetreiber und Dienstprogramme installiert werden, um sicherzustellen, dass alle Funktionen unterstützt werden und einwandfrei arbeiten.

HP hat das Auffinden, den Zugriff, die Bewertung und die Installation der neuesten Support-Software erheblich vereinfacht. Sie können die Software unter <http://www.hp.com/support> herunterladen.

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

Bausteine und Partner

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

- Desktop Management Interface (DMI) 2.0
- Wake on LAN-Technologie
- ACPI
- SMBIOS
- PXE (Pre-boot Execution)-Unterstützung

Bestandsüberwachung und Sicherheit

Die auf dem Computer vorinstallierten Bestandsüberwachungsfunktionen stellen Ihnen wichtige Daten zur Bestandsüberwachung bereit, die über HP Insight Manager, HP Client Manager oder andere Systemverwaltungsanwendungen verwaltet werden können. Die nahtlose automatische Integration in diese Produkte ermöglicht Ihnen die Auswahl des Management-Tools, das für Ihre Umgebung am besten geeignet ist, ohne Ihre bisherigen Investitionen in entsprechende Tools in Frage zu stellen.

Darüber hinaus bietet HP mehrere Lösungen zur Steuerung des Zugriffs auf wichtige Komponenten und Daten an. Sicherheitsfunktionen wie der Smart Cover Sensor und das Smart Cover Lock, die für bestimmte Modelle verfügbar sind, schützen gegen unberechtigten Zugriff auf interne Komponenten des Computers. 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 Systemverwaltungsprogramme weitergeleitet werden, um darauf aufmerksam zu machen, dass sich jemand unerlaubten Zugang zu den internen Komponenten des Computers verschafft.



Der Smart Cover Sensor und das Smart Cover Lock stehen als Zusatzoptionen für ausgewählte Systeme zur Verfügung.

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

- Lokal, mit Hilfe von Computer Setup Utility. Weitere Informationen und Anleitungen zur Verwendung dieses Dienstprogramms finden Sie im *Computer Setup (F10) Utility Handbuch*, das im Lieferumfang des Computers enthalten ist.
- Remote, mit HP Client Manager oder System Software Manager. Diese Software ermöglicht den sicheren, einheitlichen Einsatz und die Steuerung von Sicherheitseinstellungen über ein einfaches Befehlszeilen-Dienstprogramm.

Die folgende Tabelle und die folgenden Abschnitte beziehen sich auf das lokale Management von Sicherheitsfunktionen des Computers über Computer Setup Utility (F10).

Überblick über die Sicherheitsfunktionen

Funktion	Zweck	Einrichtung
Removable Media Boot Control (Start-Schutz bei Wechsellaufwerken)	Verhindert den Systemstart von einem Wechsellaufwerk aus.	Im Menü von Computer Setup Utility (F10).
Serial, Parallel, USB, or Infrared Interface Control (Steuerung von seriellen, parallelen, USB- oder Infrarotschnittstellen)	Verhindert die Datenübertragung über die serielle, parallele, USB- oder Infrarotschnittstelle.	Im Menü von Computer Setup Utility (F10).
Power-On Password (Kennwort für den Systemstart)	Verhindert den Zugriff auf den Computer bis zur Eingabe des Kennworts. Dies kann sowohl für den ersten Start als auch für einen Neustart gelten.	Im Menü von Computer Setup Utility (F10).
Setup Password (Setup-Kennwort)	Der Computer kann erst dann (über Computer Setup Utility) neu konfiguriert werden, wenn das Setup-Kennwort eingegeben wird.	Im Menü von Computer Setup Utility (F10).
DriveLock	Verhindert unbefugten Zugriff auf die Daten bestimmter Festplatten. Diese Funktion ist nur bei einigen Modellen verfügbar.	Im Menü von Computer Setup Utility (F10).



Weitere Informationen zu Computer Setup finden Sie im *Computer Setup (F10) Utility Handbuch*.

Die Unterstützung von Sicherheitsfunktionen kann je nach Computer-Konfiguration unterschiedlich sein.

Überblick über die Sicherheitsfunktionen (Fortsetzung)

Funktion	Zweck	Einrichtung
Smart Cover Sensor	Zeigt an, dass die Gehäuseabdeckung bzw. die Seitenabdeckung entfernt wurde. Kann so eingestellt werden, dass das Setup-Kennwort für den Neustart des Computers angegeben werden muss, wenn die Gehäuseabdeckung oder die Seitenabdeckung entfernt wurde. Weitere Informationen finden Sie im <i>Hardware-Referenzhandbuch</i> auf der <i>Documentation Library</i> CD. Diese Funktion ist nur bei einigen Modellen verfügbar.	Im Menü von Computer Setup Utility (F10).
Master Boot Record Security (Master Boot Record-Sicherheit)	Kann unbeabsichtigte oder böswillige Änderungen am Master Boot Record der aktuellen bootfähigen Festplatte verhindern und stellt ein Mittel zur Wiederherstellung des letzten als gut befundenen MBRs dar.	Im Menü von Computer Setup Utility (F10).
Memory Change Alerts (Warnmeldungen bei Speicheränderungen)	Erkennt, ob Speichermodule hinzugefügt, verschoben oder entfernt wurden und benachrichtigt den Benutzer sowie den Systemadministrator.	Informationen zur Aktivierung dieser Warnmeldungen finden Sie im Online-Handbuch <i>Intelligent Manageability</i> .



Weitere Informationen zu Computer Setup finden Sie im *Computer Setup (F10) Utility Handbuch*.

Die Unterstützung von Sicherheitsfunktionen kann je nach Computer-Konfiguration unterschiedlich sein.

Überblick über die Sicherheitsfunktionen (Fortsetzung)

Funktion	Zweck	Einrichtung
Eigentümerkennung	Zeigt beim Systemstart Informationen über den Eigentümer (geschützt durch das Setup-Kennwort) an, die vom Systemadministrator eingegeben wurden.	Im Menü von Computer Setup Utility (F10).
Kabelschloss	Verhindert den Zugriff auf das Innere des Computers, damit keine Änderungen an der Konfiguration vorgenommen oder Komponenten entfernt werden können. Kann auch dazu verwendet werden, den Computer an einem unbeweglichen Gegenstand zu befestigen, um ihn gegen Diebstahl zu sichern.	Bringen Sie ein Kabelschloss an, um den Computer an einem unbeweglichen Gegenstand zu befestigen.
Ringschloss	Verhindert den Zugriff auf das Innere des Computers, damit keine Änderungen an der Konfiguration vorgenommen oder Komponenten entfernt werden können.	Bringen Sie ein Ringschloss an, um zu verhindern, dass ungewollte Änderungen an der Konfiguration vorgenommen oder Komponenten entfernt werden.



Weitere Informationen zu Computer Setup finden Sie im *Computer Setup (F10) Utility Handbuch*.

Die Unterstützung von Sicherheitsfunktionen kann je nach Computer-Konfiguration unterschiedlich sein.

Kennwort-Schutz

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. Der Zugriff auf den Computer wird also gewährt, wenn bei der Eingabeaufforderung für das Kennwort für den Systemstart stattdessen das Setup-Kennwort eingegeben wird.

Ein Kennwort für das gesamte Netzwerk kann festgelegt werden, damit der Systemadministrator sich für Wartungsarbeiten bei allen Netzwerksystemen anmelden kann, ohne das Kennwort für den Systemstart zu kennen, selbst wenn dieses festgelegt wurde.

Einrichten eines Setup-Kennworts über Computer Setup

Wenn ein Setup-Kennwort über Computer Setup eingerichtet wird, können Sie den Computer nur dann über Computer Setup Utility (F10) neu konfigurieren, wenn Sie das Kennwort eingeben.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu.
Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Wenn die Meldung **F10 Setup** in der unteren rechten Bildschirmcke angezeigt wird, drücken Sie die Taste **F10**.
Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zuzugreifen.

3. Wählen Sie **Security** (Sicherheit) und anschließend **Setup Password** (Setup-Kennwort). Folgen Sie dann den Anleitungen auf dem Bildschirm.
4. Klicken Sie zum Beenden auf **File > Save Changes and Exit** (Datei > Änderungen speichern und schließen).

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. Bei der Festlegung eines Kennworts für den Systemstart zeigt Computer Setup im Sicherheitsmenü Kennwortoptionen an. Als Kennwortoptionen steht **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 > Beenden > Neu starten**.
2. Wenn die Meldung **F10 Setup** in der unteren rechten Bildschirmecke angezeigt wird, drücken Sie die Taste **F10**. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zuzugreifen.

3. Wählen Sie **Security** (Sicherheit) und anschließend **Power-On Password** (Systemstart-Kennwort). Folgen Sie dann den Anleitungen auf dem Bildschirm.
4. Klicken Sie zum Beenden auf **File > Save Changes and Exit** (Datei > Änderungen speichern und schließen).

Eingeben eines Kennworts für den Systemstart

So geben Sie ein Kennwort für den Systemstart ein:

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



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

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 > Beenden > Neu starten**.
2. Wenn die Meldung **F10 = Setup** in der unteren rechten Bildschirmecke angezeigt wird, drücken Sie die Taste **F10**.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zuzugreifen.

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



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

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**. Starten Sie **Computer Setup**, um das Setup-Kennwort zu ändern.
2. Wenn das Schlüsselsymbol angezeigt wird, geben Sie Ihr aktuelles Kennwort, einen Schrägstrich (/) oder ein anderes Begrenzungszeichen, Ihr neues Kennwort, einen weiteren Schrägstrich (/) bzw. ein anderes Begrenzungszeichen und ein zweites Mal Ihr neues Kennwort ein, so dass der Eintrag wie folgt aussieht:
aktuelles Kennwort/neues Kennwort/neues Kennwort



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

3. Drücken Sie die **Eingabetaste**.

Das neue Kennwort gilt ab dem nächsten Start des Computers.



Weitere Informationen zu Begrenzungszeichen finden Sie im Abschnitt *Begrenzungszeichen auf landesspezifischen Tastaturen* in diesem Kapitel. 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

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**. Starten Sie Computer Setup, um das Setup-Kennwort zu löschen.
2. Wenn das Schlüsselsymbol angezeigt wird, geben Sie Ihr aktuelles Kennwort und einen Schrägstrich (/) oder ein anderes Begrenzungszeichen ein (siehe unten): **aktuelles Kennwort/**
3. Drücken Sie die **Eingabetaste**.



Weitere Informationen zu Begrenzungszeichen finden Sie unter *Begrenzungszeichen auf landesspezifischen Tastaturen*. 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 Ihres Kennworts verwenden, hängen von der Anordnung der Tasten auf Ihrer Tastatur ab.

Begrenzungszeichen auf landesspezifischen Tastaturen

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

*Bosnien-Herzegowina, Kroatien, Slowenien und Jugoslawien

Löschen von Kennwörtern

Wenn Sie das Benutzerkennwort nicht mehr wissen, können Sie nicht mehr auf Ihren Computer zugreifen. Anleitungen zum Löschen von Kennwörtern finden Sie im *Fehlerbeseitigungs-Handbuch*.

DriveLock

DriveLock ist eine Sicherheitsfunktion, die den unbefugten Zugriff auf Daten bestimmter Festplatten verhindert. DriveLock wurde als Erweiterung von Computer Setup entwickelt. Diese Funktion steht nur bei einigen Systemen zur Verfügung, und zwar nur dann, wenn diese Systeme DriveLock-fähige Festplatten besitzen.

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 bei unberechtigtem Zugriff auf ihren Inhalt entstehen kann. Damit dieses hohe Sicherheitsniveau nicht zu allzu großen Problemen führt, wenn ein Kennwort vergessen wird, 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 Laufwerkssperre aufzuheben. Deshalb ist die Verwendung von DriveLock am sichersten, wenn die auf der Festplatte enthaltenen Daten in ein Firmeninformationssystem repliziert oder regelmäßig gesichert werden.

Falls beide Kennwörter für DriveLock 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 jedoch, die dem Profil entsprechen, bedeutet es im Hinblick auf die auf der Festplatte gespeicherten Daten ein Risiko, das hingenommen werden kann.

Verwenden von DriveLock

In Computer Setup ist DriveLock eine Option im Sicherheitsmenü. Dem Benutzer stehen Möglichkeiten zur Festlegung des Masterkennworts oder zur Aktivierung von DriveLock zur Verfügung. Zur Aktivierung von DriveLock muss ein Benutzerkennwort angegeben werden. Da die erste Konfiguration von DriveLock normalerweise vom Systemadministrator ausgeführt wird, sollte zuerst ein Masterkennwort festgelegt werden. HP befürwortet immer die Festlegung eines Masterkennworts durch den Administrator, unabhängig davon, ob DriveLock aktiviert werden soll. Dadurch hat der Administrator die Möglichkeit, DriveLock-Einstellungen zu ändern, wenn das Laufwerk einmal gesperrt sein sollte. Ist das Masterkennwort festgelegt, kann der Administrator DriveLock entweder aktivieren oder deaktiviert lassen.

Bei einer gesperrten Festplatte wird beim POST ein Kennwort zum Aufheben der Sperre abgefragt. Wenn ein Kennwort für den Systemstart festgelegt ist, das dem Benutzerkennwort für das Gerät entspricht, wird beim POST nicht erneut zur Eingabe des Kennworts aufgefordert. Andernfalls wird der Benutzer zur Eingabe eines DriveLock-Kennworts aufgefordert. Dabei kann entweder das Master- oder das Benutzerkennwort verwendet werden. Benutzern stehen zwei Versuche zur richtigen Kennworteingabe frei. Wird zweimal das falsche Kennwort eingegeben, wird der POST fortgesetzt, es besteht aber kein Zugriff auf Daten der Festplatte.

Anwendungen von DriveLock

Am besten ist die DriveLock-Sicherheitsfunktion für eine Firmenumgebung geeignet, in der die Computer einiger Benutzer mit Multibay Festplatten ausgestattet sind. Der Systemadministrator hat die Aufgabe, die Multibay Festplatte zu konfigurieren, das heißt unter anderem, auch das DriveLock-Masterkennwort festzulegen. Falls der Benutzer das Benutzerkennwort vergisst oder das Gerät an einen anderen Mitarbeiter weitergegeben wird, kann das Masterkennwort immer 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 wird. 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

Der Smart Cover Sensor (nur bei einigen Modellen), eine Kombination aus Hardware- und Softwaretechnologie, gibt eine Warnmeldung aus, wenn die Gehäuseabdeckung bzw. die Seitenabdeckung entfernt wurde. Es gibt drei Schutzstufen, die in der folgenden Tabelle beschrieben werden.

Schutzstufen des Smart Cover Sensors

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 auf dem Bildschirm eine Meldung darüber angezeigt, dass die Gehäuseabdeckung bzw. die Seitenabdeckung entfernt wurde.
Stufe 2	Setup Password (Setup-Kennwort)	Wenn der Computer neu gestartet wird, wird auf dem Bildschirm eine Meldung darüber angezeigt, dass die Gehäuseabdeckung bzw. die Seitenabdeckung entfernt wurde. Sie müssen das Setup-Kennwort eingeben, um fortfahren zu können.



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 stellen Sie eine Schutzstufe für den Smart Cover Sensor ein:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu.
Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Wenn die Meldung **F10 Setup** in der unteren rechten Bildschirmecke angezeigt wird, drücken Sie die Taste **F10**. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zuzugreifen.

3. Wählen Sie **Security** (Sicherheit) und anschließend **Smart Cover**. Folgen Sie dann den Anleitungen auf dem Bildschirm.
4. Klicken Sie zum Beenden auf **File > Save Changes and Exit** (Datei > Änderungen speichern und schließen).

Smart Cover Lock

Das Smart Cover Lock ist eine über die Software gesteuerte Abdeckungsverriegelung, mit der einige HP Computer ausgestattet sind. Sie verhindert den unbefugten Zugriff auf die inneren Komponenten des Computers. Die Computer werden mit deaktiviertem Smart Cover Lock geliefert.



ACHTUNG: Für die maximale Sicherheit der Abdeckungsverriegelung müssen Sie ein Setup-Kennwort einrichten. Das Setup-Kennwort verhindert den unbefugten Zugriff auf Computer Setup.



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

Aktivieren des Smart Cover Lock

So aktivieren Sie die Sperrfunktion des Smart Cover Lock:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu.
Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Wenn die Meldung **F10 Setup** in der unteren rechten Bildschirmecke angezeigt wird, drücken Sie die Taste **F10**.
Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zuzugreifen.

3. Wählen Sie **Security** (Sicherheit), dann **Smart Cover** und anschließend die Option **Locked** (Gesperrt).
4. Klicken Sie zum Beenden auf **File > Save Changes and Exit** (Datei > Änderungen speichern und schließen).

Aufheben der Sperre des Smart Cover Lock

1. Schalten Sie den Computer ein, oder starten Sie ihn neu.
Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Wenn die Meldung **F10 Setup** in der unteren rechten Bildschirmecke angezeigt wird, drücken Sie die Taste **F10**. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zuzugreifen.

3. Wählen Sie **Security > Smart Cover > Unlocked** (Sicherheit > Smart Cover > Sperre aufgehoben).
4. Klicken Sie zum Beenden auf **File > Save Changes and Exit** (Datei > Änderungen speichern und schließen).

Verwenden des Smart Cover FailSafe-Schlüssels

Wenn das Smart Cover Lock aktiviert ist und Sie Ihr 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)
- Kennwort vergessen



ACHTUNG: Der Smart Cover FailSafe-Schlüssel ist ein spezielles Tool, das von HP angeboten wird. Vermeiden Sie lange Ausfallzeiten bei unliebsamen Überraschungen, und bestellen Sie den Schlüssel bei einem Servicepartner.

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

- Wenden Sie sich an Ihren HP Partner oder Servicepartner.
- Rufen Sie die in der Garantieerklärung genannte Rufnummer an.

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

Master Boot Record Security (Master Boot Record-Sicherheit)

Der Master Boot Record (MBR) enthält Informationen, die für den erfolgreichen Start von einer Diskette aus und den Zugriff auf die auf der Diskette gespeicherten Daten erforderlich sind. Mit Hilfe von Master Boot Record Security können unbeabsichtigte oder böswillige Änderungen am MBR verhindert werden, die beispielsweise durch Viren oder die unkorrekte Verwendung von bestimmten Festplattendienstprogrammen verursacht werden. Sie haben außerdem die Möglichkeit, den letzten als gut befundenen MBR wiederherzustellen, wenn Sie beim Neustart des Systems Änderungen am MBR feststellen.

So aktivieren Sie die MBR-Sicherheit:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu.
Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Wenn die Meldung **F10 Setup** in der unteren rechten Bildschirmcke angezeigt wird, drücken Sie die Taste **F10**. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zuzugreifen.

3. Wählen Sie **Security > Master Boot Record Security > Enabled** (Sicherheit > Master Boot Record-Sicherheit > Aktiviert).
4. Wählen Sie **Security > Save Master Boot Record** (Sicherheit > Master Boot Record speichern).
5. Klicken Sie zum Beenden auf **File > Save Changes and Exit** (Datei > Änderungen speichern und schließen).

Wenn die MBR-Sicherheit aktiviert ist, verhindert das BIOS sämtliche Änderungen am MBR der aktuellen bootfähigen Festplatte, solange in MS-DOS oder Windows der geschützte Modus aktiviert ist.



Die meisten Betriebssysteme steuern den Zugriff auf den MBR der aktuellen bootfähigen Festplatte. Das BIOS kann keine Änderungen verhindern, die während der Ausführung des Betriebssystems erfolgen.

Bei jedem Einschalten oder Neustart des Computers vergleicht das BIOS den MBR der aktuellen bootfähigen Festplatte mit dem zuvor gespeicherten MBR. Wenn Änderungen festgestellt werden und wenn es sich bei der aktuellen bootfähigen Festplatte um dieselbe Festplatte handelt, von welcher der MBR zuvor gespeichert wurde, wird die folgende Meldung angezeigt:

1999 – Master Boot Record has changed (1999 – Master Boot Record wurde geändert).

Press any key to enter Setup to configure MBR Security.
(Drücken Sie eine beliebige Taste, um Computer Setup zu starten und die MBR-Sicherheit zu konfigurieren.)

Wenn Sie Computer Setup starten, müssen Sie die folgenden Aktionen durchführen:

- Speichern des MBR der aktuellen bootfähigen Festplatte
- Wiederherstellen des zuvor gespeicherten MBR oder
- Deaktivieren der MBR-Sicherheitsfunktion.

Sie benötigen das Setup-Kennwort, falls ein Kennwort eingerichtet wurde.

Wenn Änderungen festgestellt werden und wenn es sich bei der aktuellen bootfähigen Festplatte **nicht** um dieselbe Festplatte handelt, von der der MBR zuvor gespeichert wurde, wird die folgende Meldung angezeigt:

2000 – Master Boot Record Hard Drive has changed (Die Master Boot Record-Festplatte wurde geändert).

Press any key to enter Setup to configure MBR Security.
(Drücken Sie eine beliebige Taste, um Computer Setup zu starten und die MBR-Sicherheit zu konfigurieren.)

Wenn Sie Computer Setup starten, müssen Sie die folgenden Aktionen durchführen:

- Speichern des MBR der aktuellen bootfähigen Festplatte oder
- Deaktivieren der MBR-Sicherheitsfunktion.

Sie benötigen das Setup-Kennwort, falls ein Kennwort eingerichtet wurde.

In dem unwahrscheinlichen Fall, dass der zuvor gespeicherte MBR beschädigt wurde, wird die folgende Meldung angezeigt:

1998 – Master Boot Record has been lost (1998 – Master Boot Record ist verloren gegangen).

Press any key to enter Setup to configure MBR Security.
(Drücken Sie eine beliebige Taste, um Computer Setup zu starten und die MBR-Sicherheit zu konfigurieren.)

Wenn Sie Computer Setup starten, müssen Sie die folgenden Aktionen durchführen:

- Speichern des MBR der aktuellen bootfähigen Festplatte oder
- Deaktivieren der MBR-Sicherheitsfunktion.

Sie benötigen das Setup-Kennwort, falls ein Kennwort eingerichtet wurde.

Maßnahmen vor der Partitionierung oder Formatierung der aktuellen bootfähigen Festplatte

Stellen Sie sicher, dass die MBR-Sicherheit deaktiviert ist, bevor Sie die Formatierung oder Partitionierung der aktuellen bootfähigen Festplatte ändern. Einige Festplattendienstprogramme (wie z. B. FDISK und FORMAT) versuchen, den MBR zu aktualisieren. Wenn die MBR-Sicherheit aktiviert ist, während Sie die Partitionierung oder Formatierung der Festplatte ändern, erhalten Sie beim nächsten Start oder Neustart des Computers möglicherweise Fehlermeldungen vom Festplattendienstprogramm oder einen Warnhinweis von MBR Security. Führen Sie die folgenden Schritte durch, um MBR Security zu deaktivieren:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu.
Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Wenn die Meldung **F10 Setup** in der unteren rechten Bildschirmecke angezeigt wird, drücken Sie die Taste **F10**. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zuzugreifen.

3. Wählen Sie **Security > Master Boot Record Security > Disabled** (Sicherheit > Master Boot Record-Sicherheit > Deaktiviert).
4. Klicken Sie zum Beenden auf **File > Save Changes and Exit** (Datei > Änderungen speichern und schließen).

Kabelschloss

Die Anbringung eines Kabelschlosses ist auf der Rückseite des Computers möglich, so dass dieser an einem festen Gegenstand angeschlossen werden kann.

Anleitungen mit den entsprechenden Abbildungen finden Sie im *Hardware-Referenzhandbuch* auf der *Documentation Library* CD.

Fingerprint Identification Technology

Die HP Fingerprint Identification Technology macht die Eingabe eines Benutzerkennworts überflüssig, erhöht die Netzwerksicherheit, vereinfacht den Anmeldevorgang 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.



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

Weitere Informationen finden Sie unter folgender Adresse:
<http://www.compaq.com/solutions/security>

Fehlermeldung und Fehlerbehebung

Die Funktionen zur Fehlermeldung und Fehlerbehebung sorgen durch die Kombination innovativer Hardware- und Softwaretechnologien dafür, dass der Verlust wichtiger Daten verhindert Ausfälle vermieden werden können.

Im Falle eines Fehlers gibt der Computer eine Warnmeldung aus, die den Fehler beschreibt und Vorsichtsmaßnahmen empfiehlt. Sie können sich dann den aktuellen Zustand des Systems über HP Client Manager anzeigen lassen. Wenn der Computer an ein Netzwerk angeschlossen ist, das von HP Insight Manager, HP Client Manager oder einem anderen Systemverwaltungsprogramm überwacht wird, sendet der Computer auch an die Netzwerk-Management-Anwendung eine Fehlermeldung.

Drive Protection System

Das Drive Protection System (DPS) ist ein in die Festplatten bestimmter HP Computer integriertes Diagnose-Tool. Dieses Tool soll die Diagnostizierung von Problemen unterstützen, die zu einem Festplattenaustausch führen könnten.

Jede Festplatte wird vor dem Einbau in einen HP Computer unter Verwendung von DPS getestet, und wichtige Informationen werden permanent auf der Festplatte gespeichert. Die Testergebnisse werden bei jeder Ausführung von DPS auf der Festplatte gespeichert. Anhand dieser Informationen kann Ihr Servicepartner unter Umständen eine Diagnose der Bedingungen erleichtern, aufgrund derer Sie DPS ausgeführt haben. Hinweise zur Verwendung von DPS finden Sie im *Fehlerbeseitigungs-Handbuch*.

Überspannungsschutz

Ein integriertes überspannungstolerantes Netzteil bietet eine größere Zuverlässigkeit, wenn der Computer einer unvorhergesehen hohen Spannung ausgesetzt wird. Dieses Netzteil ist so ausgelegt, dass eine Überspannung von bis zu 2000 V ohne Systemausfall oder Datenverluste neutralisiert werden kann.

Thermosensor

Der Thermosensor ist eine Hard- und Softwarefunktion zur Messung der Innentemperatur eines Computers. Diese Funktion zeigt eine Warnmeldung an, wenn der normale Temperaturbereich überschritten wird, so dass Sie Maßnahmen ergreifen können, bevor die internen Komponenten beschädigt werden oder Daten verloren gehen.

Index

A

- Abdeckungsverriegelung, Smart Cover Lock 29
- Abdeckungsverriegelung, Vorsichtsmaßnahmen 29
- ActiveUpdate 8
- Aktivieren des Smart Cover Lock 30
- Aktualisieren des ROM-Speichers 8
- Altiris eXpress 4
- Altiris eXpress PC Transplant Pro 6
- Ändern des Betriebssystems, Wichtige Informationen 15
- Ändern des Kennworts 23
- Anpassen der Software 2

B

- Begrenzungszeichen 24
- Bestandsüberwachung 16
- Bestellen eines FailSafe-Schlüssels 31
- Betriebssysteme, Wichtige Informationen 15
- Bootfähige Festplatte, Wichtige Informationen 34

C

- Cloning-Tools, Software 2
- Computer Setup Utility 12

D

- Deaktivieren des Smart Cover Lock 30
- Diagnose-Tool für Festplatten 36
- Dual-State-Netzschalter 13

E

- Eingeben
 - Kennwort für Systemstart 22
 - Setup-Kennwort 22
- Einrichten
 - Setup-Kennwort 20, 22
- Einsatz-Tools, Software 2
- Einstellen
 - Smart Cover Sensor 29
- Einstellung
 - Timeouts 14
- Energiesparen, Einstellungen 14
- Erste Konfiguration 2

F

- FailSafe Boot Block ROM 10
- FailSafe-Schlüssel
 - Bestellen 31
 - Vorsichtsmaßnahmen 31
- Fehlermeldung 36
- Festplatte, Cloning 2
- Festplatten, Diagnose-Tool 36
- Fingerprint Identification Technology 35
- Formatieren der Festplatte, Wichtige Informationen 34

H

- HP Client Manager 6

I

- Interne Temperatur des Computers 37
- Internetadressen. Siehe Websites

K

Kabelschloss 35

Kennwort

Ändern 23

Löschen 23, 24

Setup 20, 22

Systemstart 22

Kennwort für Systemstart

Ändern 23

Löschen 23

Kennwortschutz 20

Konfigurieren des Netzschalters 13

Kontrollieren des Computerzugriffs 16

L

Landesspezifische Unterschiede bei

Begrenzungszeichen 24

Laufwerk, Schützen 36

Löschen des Kennworts 23

Löschen von Kennwörtern 24

M

Master Boot Record Security, Einstellen 32

N

Netzschalter

Dual-State 13

Konfigurieren 13

Netzteil, Überspannungstolerant 37

P

Partitionieren der Festplatte, Wichtige

Informationen 34

Power Management 14

Preboot Execution Environment (PXE) 3

PXE (Preboot Execution Environment) 3

R

Remote ROM Flash 9

Remote System Installation, Zugriff 3

Remote-Installation 3

ROM, Aktualisieren 8

ROM, Ungültig 9

ROM-Tastatur-LEDs, Tabelle 11

S

Schutz des ROM-Speichers,

Vorsichtsmaßnahmen 8

Schützen der Festplatten 36

Setup, beim ersten Start 2

Setup, Replizieren 12

Setup-Kennwort

Eingeben 22

Einrichten 20

Löschen 23

Sicherheit, Master Boot Record 32

Sicherheitseinstellungen, Einrichtung 16

Sicherheitsfunktionen, Tabelle 17

Smart Cover FailSafe-Schlüssel, Bestellen 31

Smart Cover Lock

Aktivieren 30

Deaktivieren 30

Smart Cover Sensor

Einstellen 29

Schutzstufen 28

Software

Aktualisieren mehrerer Computer 7

Altiris eXpress 4

Bestandsüberwachung 16

Computer Setup Utility 12

Drive Protection System 36

FailSafe Boot Block ROM 10

Fehlermeldung und Fehlerbehebung 36

Integration 2

Master Boot Record-Sicherheit 32

Power Management 14

Remote ROM Flash 9

Remote System Installation 3

System Software Manager 7

Wiederherstellung 2

Sparen von Energie 14
SSM (System Software Manager) 7
System Software Manager (SSM) 7
Systemstart-Kennwort
 Eingeben 22
Systemwiederherstellung 9

T

Tabelle 24
Tastatur-Begrenzungszeichen,
 Landesspezifische Unterschiede 24
Tastatur-LEDs, ROM, Tabelle 11
Temperatur, Im Computer 37
Thermosensor 37
Timeouts, Einstellung 14

U

Überspannungsschutz 37
Ungültiger System-ROM-Speicher 9
URLs (Websites). Siehe Websites

V

Vorinstalliertes Software-Image 2

Vorsichtsmaßnahmen
 Abdeckungsverriegelung 29
 FailSafe-Schlüssel 31
 Schutz des ROM-Speichers 8

W

Web-Adressen. Siehe Websites

Websites

www.compaq.com/activeupdate 8
www.compaq.com/easydeploy 5, 6, 9, 12
www.compaq.com/im/ssmwp.html 7, 8
www.compaq.com/solutions/
 pc solutions 2
www.compaq.com/solutions/security 35
www.hp.com/support 8, 15
www.hp.com/united-states/subscribe 7

Wiederherstellen des Systems 9

Wiederherstellung, Software 2

Z

Zugriff auf Computer, Kontrollieren 16