



# **Desktop Management**

## Business PCs

Dokument-Teilenummer: 391759-041

**Mai 2005**

Dieses Handbuch enthält Definitionen und Anleitungen zur Verwendung der Funktionen für Sicherheit und Intelligent Manageability, über die einige Modelle verfügen.

© Copyright 2005 Hewlett-Packard Development Company, L.P.  
Inhaltliche Änderungen dieses Dokuments behalten wir uns ohne Ankündigung vor. Die Informationen in dieser Veröffentlichung werden ohne Gewähr für ihre Richtigkeit zur Verfügung gestellt. Insbesondere enthalten diese Informationen keinerlei zugesicherte Eigenschaften. Alle sich aus der Verwendung dieser Informationen ergebenden Risiken trägt der Benutzer.

Microsoft und Windows sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

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. Hewlett-Packard („HP“) haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument. Ferner übernimmt sie keine Haftung für Schäden, die direkt oder indirekt auf die Bereitstellung, Leistung und Nutzung dieses Materials zurückzuführen sind. Die Haftung für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer fahrlässigen Pflichtverletzung durch HP oder einer vorsätzlichen oder fahrlässigen Pflichtverletzung eines gesetzlichen Vertreters oder Erfüllungsgehilfen von HP beruhen, bleibt hierdurch unberührt. Ebenso bleibt hierdurch die Haftung für sonstige Schäden, die auf einer grob fahrlässigen Pflichtverletzung durch HP oder auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung eines gesetzlichen Vertreters oder Erfüllungsgehilfen von HP beruht, unberührt.

Dieses Dokument enthält urheberrechtlich geschützte Informationen. Ohne schriftliche Genehmigung der Hewlett-Packard Company darf dieses Dokument weder kopiert noch in anderer Form vervielfältigt oder übersetzt werden.



**VORSICHT:** In dieser Form gekennzeichnete Text weist auf Verletzungs- oder Lebensgefahr bei Nichtbefolgen der Anleitungen hin.

---



**ACHTUNG:** Kennzeichnet eine Anweisung, deren Nichtbeachtung zur Beschädigung von Komponenten oder zum Verlust von Daten führen kann.

---

## **Desktop Management**

Business PCs

Erste Ausgabe (Mai 2005)

**Dokument-Teilenummer: 391759-041**

## Desktop Management

Erste Konfiguration und Implementierung .....	2
Altiris Deployment Solution Agent .....	3
HP Local Recovery .....	3
Remote System Installation .....	4
Software-Aktualisierung und -Management .....	5
HP System Software Manager .....	5
HP Client Manager Software .....	6
HP Client Management Solutions using Altiris .....	7
HP OpenView Management Suite for Desktops using Radia .....	8
HP Local Recovery .....	10
Dantz Retrospect Express .....	11
Proactive Change Notification .....	12
Subscriber's Choice .....	13
Ehemalige Lösungen .....	13
ROM-Flash .....	14
Remote ROM Flash .....	14
HPQFlash .....	15
Boot-Block-Wiederherstellungsmodus .....	15
Replizieren des Setup .....	16
Dual-State-Netzschalter .....	25
HP Website .....	26
Bausteine und Partner .....	26
Bestandsüberwachung und Sicherheit .....	27
Kennwort-Schutz .....	31
Einrichten eines Setup-Kennworts über Computer Setup .....	31
Einrichten des Kennworts für den Systemstart über Computer Setup .....	32
DriveLock .....	37
Smart Cover Sensor .....	39

Smart Cover Lock .....	40
Diebstahlsicherung .....	42
Fingerabdruckerkennungstechnologie .....	42
Fehlermeldung und Fehlerbeseitigung .....	43
Drive Protection System .....	43
Überspannungsschutz .....	44
Thermosensor .....	44

## **Index**

---

# Desktop Management

HP Client Management Solutions bietet standardbasierte Lösungen für das Management und die 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 Desktop Manageability und ist Inhaber von Patenten für Manageability-Technologie. Seitdem ist HP branchenweit bemüht, die Standards und die Infrastruktur zu entwickeln, die für eine effektive Implementierung, Konfiguration und das Management von Desktops, Workstations und Notebook-PCs erforderlich sind. HP arbeitet eng mit branchenführenden Anbietern von Management-Softwarelösungen zusammen, um die Kompatibilität zwischen Client Management Solutions und diesen Produkten sicherzustellen. HP Client Management Solutions ist eine wichtige Komponente des umfassenden Engagements von HP, PC Lifecycle-Lösungen für alle vier Phasen des Lebenszyklus eines Desktop-PCs anzubieten – von der Planung, Implementierung und dem Management bis hin zu Umstellungen.

Die wichtigsten Merkmale und Funktionen von Desktop Management sind:

- Erste Konfiguration und Implementierung
- Remote System Installation
- Software-Aktualisierung und -Management
- ROM-Flash
- Bestandsüberwachung und Sicherheit
- Fehlermeldung und Fehlerbeseitigung



---

Die Unterstützung von bestimmten, in diesem Handbuch beschriebenen Funktionen kann je nach Modell oder Software-Version unterschiedlich sein.

---

## Erste Konfiguration und Implementierung

Der Computer wird 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. Beispiele:

- Installation zusätzlicher Software-Anwendungen nach dem Auspacken des vorinstallierten Software-Images
- Verwendung von Software-Implementierungs-Tools, wie etwa Altiris Deployment Solution, um die vorinstallierte Software durch ein benutzerdefiniertes Software-Image zu ersetzen
- Verwendung eines Disk-Cloning-Verfahrens zum Kopieren des Inhalts einer Festplatte auf eine andere

Welche Implementierungsmethode am besten geeignet ist, hängt von Ihrer IT-Umgebung und den damit verbundenen Prozessen ab. Informationen zur Wahl der am besten geeigneten Implementierungsmethode finden Sie im Abschnitt „PC Deployment“ auf der Website für HP Lifecycle-Lösungen unter (<http://whp-sp-orig.extweb.hp.com/country/us/en/solutions.html>).

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

## Altiris Deployment Solution Agent

Dieses Programm ist bereits auf der Festplatte gespeichert. Es ermöglicht die Kommunikation mit der Deployment Solution-Administratorkonsole.

So installieren Sie Altiris Deployment Solution Agent:

1. Klicken Sie auf **Start**.
2. Klicken Sie auf **Alle Programme**.
3. Wählen Sie dann **Software Setup** (Software-Setup).
4. Klicken Sie auf **Next** (Weiter).
5. Blättern Sie nach unten, und klicken Sie auf die Verknüpfung, um Altiris Aclient zu installieren.

## HP Local Recovery

Mit Local Recovery werden Daten- und Systemdateien in einem geschützten Bereich auf der Festplatte gesichert. Falls Daten oder Dateien verloren gehen, gelöscht werden oder beschädigt sind, können sie mithilfe von Local Recovery wieder abgerufen werden, oder es kann das letzte verwendbare System-Image wiederhergestellt werden.

So installieren Sie das bereits auf der Festplatte gespeicherte Programm:

1. Klicken Sie auf **Start**.
2. Klicken Sie auf **Local Recovery**.
3. Klicken Sie auf **Next** (Weiter).
4. Blättern Sie nach unten, und klicken Sie auf die Verknüpfung, um HP Local Recovery zu installieren.

## Remote System Installation

Remote System Installation ermöglicht Ihnen, das System mithilfe der Software und der Konfigurationsinformationen von einem Netzwerk-Server aus zu starten und einzurichten, indem Sie PXE (Preboot Execution Environment) initialisieren. Die Funktion Remote System Installation wird normalerweise als Tool zur Systemeinrichtung und -konfiguration verwendet. Darüber hinaus können jedoch auch folgende Aufgaben ausgeführt werden:

- Formatieren eines Festplattenlaufwerks
- Implementieren eines Software-Images auf einem oder mehreren neuen PCs
- Remote-Aktualisierung des System-BIOS im Flash-ROM („Remote ROM Flash“ auf Seite 14)
- Konfigurieren der Einstellungen des System-BIOS

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 des HP Logo-Bildschirms erscheint. Folgen Sie den Anleitungen auf dem Bildschirm, um fortzufahren. Die standardmäßige Startreihenfolge ist eine BIOS-Konfigurationseinstellung, die so eingestellt werden kann, dass immer ein PXE-Start über das Netzwerk versucht wird.

HP und Altiris bieten gemeinsam Tools an, die die Implementierung und das Management von Firmen-PCs vereinfachen und weniger zeitaufwendig gestalten, die Total Cost of Ownership senken und PCs von HP in der Unternehmensumgebung zu Client-PCs mit optimaler Manageability machen.

# Software-Aktualisierung und -Management

HP bietet mehrere Tools für das Management und die Aktualisierung von Software auf Desktops, Workstations und Notebooks an:

- HP System Software Manager
- HP Client Manager Software
- HP Client Management Solutions using Altiris
- HP OpenView Management Suite for Desktops using Radia
- HP Local Recovery
- Dantz Backup and Recovery
- HP Proactive Change Notification
- HP Subscriber's Choice

## HP System Software Manager

HP System Software Manager (SSM) ist ein kostenloses Utility, mit dem die Implementierung von Gerätetreibern und BIOS-Aktualisierungen auf HP Business PCs, die in ein Netzwerk eingebunden sind, automatisiert werden kann. Wenn SSM ausgeführt wird, bestimmt es ohne Benutzereingriff die Versionen von Treibern und dem BIOS, die auf jedem Netzwerk-Client-System installiert sind, und vergleicht diese Daten mit den getesteten Systemsoftware-SoftPaqs im zentralen Dateispeicher. SSM aktualisiert anschließend automatisch die Netzwerk-Computer, auf denen eine Systemsoftware vorhanden ist, die nicht der neuesten Version im zentralen Dateispeicher entspricht. Da SSM die Verteilung von SoftPaq Aktualisierungen nur für die richtigen Client-System-Modelle zulässt, können Administratoren die Systemsoftware mit SSM sicher und effizient auf dem neuesten Stand halten.

System Software Manager kann mit Software-Verteilungstools für Unternehmen, wie HP OpenView Management Suite using Radia und Microsoft Systems Management Server (SMS), eingesetzt werden. Mit SSM können kundeneigene Aktualisierungen oder Aktualisierungen von anderen Anbietern, die im SSM-Format vorliegen, verteilt werden.

SSM kann unter [www.hp.com/go/ssm](http://www.hp.com/go/ssm) kostenlos heruntergeladen werden.

## HP Client Manager Software

HP Client Manager Software using Altiris steht für alle unterstützten HP Business Desktops, Notebooks und Workstations kostenlos zur Verfügung. SSM ist in HP Client Manager integriert und ermöglicht die zentrale Verfolgung, Überwachung und das Management von Hardware auf HP Client-Systemen.

HP Client Manager bietet folgende Funktionen:

- Abrufen wertvoller Hardware-Information zu CPU, Speicher, Grafikkarte und Sicherheitseinstellungen
- Überwachen des Systemzustands, um Probleme zu beheben, bevor sie entstehen
- Installieren von Treiber- und BIOS-Aktualisierungen, ohne an jedem PC anwesend sein zu müssen
- Remote-Konfiguration von BIOS- und Sicherheitseinstellungen
- Automatisieren von Prozessen, um Hardwareprobleme schnell zu lösen

HP Client Manager verwendet die gleiche Altiris Infrastruktur wie andere Altiris Client Lifecycle Management-Lösungen. Dies bietet einen erheblichen Vorteil für die IT-Mitarbeiter, da nur eine Infrastruktur eingerichtet und verwaltet werden muss. Da die Informationen in einer Datenbank gespeichert sind, können einheitliche Bestandsberichte sowie Informationen zum Systemzustand und zur Sicherheit vollständig abgerufen werden. Über eine einzige, einheitliche Konsolenoberfläche werden Hardware- und Software-Management-Aufgaben für die Client-Systeme geplant und verfolgt.

Weitere Informationen zum HP Client Manager finden Sie unter [www.hp.com/go/easydeploy](http://www.hp.com/go/easydeploy).

## HP Client Management Solutions using Altiris

Weitere Altiris Client Management-Lösungen, die die Hardware-Management-Funktionen von HP Client Manager ergänzen, können bei HP erworben werden. Mit diesen Lösungen können folgende Aufgaben im IT-Lifecycle erledigt werden:

- Bestands-Management
- Einhaltung von Softwarelizenzbestimmungen
- Personality-Migration
- Implementierung von Software-Images
- Software-Verteilung
- Asset-Management
- Client-Datensicherung und -Wiederherstellung
- Problemlösung

Weitere Informationen zu HP Client Management Solutions using Altiris finden Sie unter [www.hp.com/go/easydeploy](http://www.hp.com/go/easydeploy).

HP und Altiris bilden eine weit über Verkaufs- und Marketing-Überlegungen hinausgehende einzigartige Allianz, die sich durch gemeinsame Entwicklungen und Austausch von Technologie auszeichnet und die Gruppen HP Client, Server, OpenView und Services umfasst. HP Partnern und Kunden können somit die besten Lösungen geboten werden.

Im Jahr 1999 haben sich die Compaq Personal Systems Group und Altiris zusammengeschlossen, um das Fachwissen von Compaq als Vorreiter im Bereich Hardware und Verwaltbarkeit von PCs und von Altiris im Bereich Implementierung und Migration zu vereinen. Aus dieser Beziehung entwickelte sich mit der Einführung von umfassenden kostenreduzierenden IT-Lifecycle-Management-Lösungen, wie der gemeinsam entwickelten HP Client Manager Software, eine strategische Allianz, die optimale Hardware-Management-Funktionen für HP PCs bietet.

Aufbauend auf dem Erfolg der Personal Systems Group hat die Industry Standard Servers Group im Jahre 2001 das ProLiant Essentials Rapid Deployment Pack auf den Markt gebracht, eine Kombination aus der OEM-Version von Altiris Deployment Solution und des HP SmartStart Toolkit. Auf der Grundlage dieser Lösung hat HP die HP ProLiant Server (einschließlich Blade Server) sowie die Blade PCs, eine Kernkomponente der HP Consolidated Client Infrastructure.

Nach dem Zusammenschluss von HP und Compaq ist diese Allianz weiter gewachsen und bietet folgende Vorteile:

- Altiris Deployment Solution kann 30 Tage lang kostenlos für HP Business PCs getestet werden. Nach diesem Zeitraum muss eine Lizenz erworben werden.
- HP Local Recovery, ein Dienstprogramm zur Client-Datensicherung und – Wiederherstellung, wird für HP Business PCs kostenlos angeboten.
- Mit Altiris Connector for HP OpenView wird die Client-Bestands- und Ereignisintegration mit HP OpenView Network Node Manager, Operations und Service Desk zur Verfügung gestellt.
- Altiris Connector for HP Systems Insight Manager ermöglicht die vereinfachte Implementierung und das Management von HP Clients und Servern über die HP Systems Insight Manager-Konsole.

HP nimmt durch seine Management-Lösung und -Konsole zur Implementierung und Konfiguration von PCs, Handhelds, Thin Clients und Windows- und Linux-Servern sowie durch die umfassende Integration mit HP Management-Tools für Unternehmen eine marktführende Rolle sein. HP bietet selbst als auch über Altiris umfangreiche Schulungs- und Serviceangebote an. Die Kombination aus HP Client Management Solutions und Servicefunktionen stellt die beste Möglichkeit für Kunden dar, die Kosten und den Aufwand für das Management von Client-Systemen zu reduzieren.

## **HP OpenView Management Suite for Desktops using Radia**

HP OpenView Management Suite for Desktops using Radia ist eine extrem skalierbare, auf Richtlinien basierende Change-Management- und Configuration-Management-Software, mit der Administratoren Software und Inhalte auf verschiedenartigen Desktop-Plattformen mithilfe einer webbasierten Konsole effizient und zuverlässig bestandsmäßig festhalten, implementieren und verwalten können.

HP OpenView Management Suite for Desktops using Radia gewährleistet die Verfügbarkeit von Desktop-Anwendungen und die Zuverlässigkeit von Betriebssystemen, Anwendungen und Inhalten, die Mitarbeiter, Partner oder Kunden benötigen.

Das Programm hat sich weltweit bewährt, da es eine Zuverlässigkeit von mehr als 99% bei der Implementierung in hochkomplexen und großmaßstäbigen IT-Umgebungen garantiert. Die Automatisierung des Change-Managements führt zu einer enormen Kostenreduzierung im IT-Bereich, einer schnelleren Markteinführung von Software und Inhalten sowie zu einer verbesserten Produktivität und größerer Zufriedenheit.

HP OpenView Management Suite for Desktops using Radia bietet folgende Vorteile:

- Plattformübergreifendes Überwachen des Hardware- und Softwarebestands
- Vorbereiten eines Anwendungspakets und Durchführen von Auswirkungsanalysen vor der Verteilung
- Auswählen einzelner Desktops, Workgroups oder des ganzen Desktopbestands, für die die Implementierung und Aktualisierung von Software und Inhalten entsprechend den Richtlinien durchgeführt werden soll
- Bereitstellen und Verwalten von Betriebssystemen, Anwendungen und Inhalten auf verteilten Desktop-Computern an einem beliebigen Standort
- Integration von HP OpenView Service Desk mit anderen Help Desk- und System-Management-Tools
- Wirksames Einsetzen einer allgemeinen Infrastruktur für das Management von Software und Inhalten auf praktisch jedem Gerät, jeder Plattform und jedem Netzwerk für alle Benutzer des Unternehmens
- Skalierbar zur Erfüllung der Anforderungen des Unternehmens

HP OpenView Management Suite for Desktops using Radia wird als eigenständige Lösung angeboten und kann als wesentliche Komponente des einzigartigen HP Desired-State-Management-Ansatzes vollständig in andere HP OpenView Management Suite using Radia-Produkte integriert werden. Dadurch wird die Software auf den einzelnen Computing-Geräten des Unternehmens automatisch und laufend verwaltet. Die HP OpenView Management Suite using Radia-Produkte gewährleisten, dass sich die komplette Software-Infrastruktur immer im gewünschten Zustand befindet – auf dem neuesten Stand, zuverlässig und sicher.

Weitere Informationen zu HP OpenView Management Suite for Desktops using Radia finden Sie unter [http://managementsoftware.hp.com/products/radia\\_mdsk/index.html](http://managementsoftware.hp.com/products/radia_mdsk/index.html).

## HP Local Recovery

Mit Local Recovery werden Datei- und Systemdateien auf HP Business Desktops, Notebooks und Workstations geschützt. Außerdem ist eine schnelle Wiederherstellung von Daten und Wiederaufnahme der Arbeit möglich, falls Informationen versehentlich gelöscht wurden oder das Betriebssystem beschädigt ist. Local Recovery wurde für Benutzer entwickelt, die gar nicht oder nur gelegentlich im Netzwerk arbeiten, und schützt die Daten auf dem HP Computer und den Systemstatuts über zeitgesteuerte, in einem geschützten Bereich auf der lokalen Festplatte gespeicherte Snapshots. Die Sicherung oder Wiederherstellung kann durch einfaches Klicken mit der Maus oder durch Drücken der Taste **F11** vor dem Booten des Betriebssystems durchgeführt werden. Die Sicherung von Systemdaten und die Wiederherstellung im Notfall kann nun von jedem Benutzer ungeachtet der Verbindung vorgenommen werden.

Local Recovery wird für HP Business PCs kostenlos zur Verfügung gestellt. Es sind außerdem zwei weitere Produkte zur Client-Wiederherstellung verfügbar. Durch den Erwerb dieser Produkte werden weitere Wiederherstellungsfunktionen zur Verfügung gestellt:

- **Local Recovery Pro:** Dieses Programm enthält alle Funktionen von Local Recovery und bietet darüber hinaus Sicherungs- und Wiederherstellungsfunktionen für eine zweite Festplatte sowie für geöffnete und gesperrte Dateien. Während der Erstellung eines Sicherungs-Snapshots werden die Informationen in geöffneten Anwendungen, wie E-Mail-Nachrichten, Präsentationen und Dokumente aus Textverarbeitungsanwendungen durch die Unterstützung von geöffneten/gesperrten Dateien beibehalten.
- **Recovery Solution:** Über eine zentrale Administrator-Konsole können vollständige Sicherungen auf Unternehmensebene und die Wiederherstellung von PCs vorgenommen werden. Datensicherungen in einem geschützten Bereich auf der lokalen Festplatte sowie in einem Speicherbereich im Netzwerk werden ebenfalls unterstützt. Diese netzwerkbasierte Wiederherstellungsfunktion bietet ein hohes Maß an Schutz vor Datenverlust aufgrund von Festplattenausfällen oder gestohlenen und falsch platzierten PCs.

Weitere Informationen zu HP Local Recovery finden Sie unter [www.hp.com/go/easydeploy](http://www.hp.com/go/easydeploy).

## **Dantz Retrospect Express**

Dantz Retrospect Express schützt einen Windows-Desktop-Computer oder ein Windows-Notebook. Mit Retrospect Express ist eine Wiederherstellung von Daten möglich, die aufgrund von Viren, neu installierter Software, Benutzerfehlern, beschädigter Hardware, Hardware-Upgrades, Hackern und verlorenen oder gestohlenen Computern verloren gegangen sind. Sie können zwischen einer einfachen Duplizierung oder einer umfassenden Sicherung wählen. Ein benutzerfreundlicher Setup-Assistent ermöglicht die Einrichtung in Minutenschnelle. Mit Retrospect Express und der in das Produkt integrierten Notfall-Wiederherstellung sind Sie bestmöglichst geschützt. Klicken Sie hier, um die Hardware-Hersteller anzuzeigen, die Retrospect in ihren Produkten verwenden. Hier finden Sie auch Angaben, wo diese Produkte erworben werden können.

Installieren Sie Retrospect Express, und führen Sie Ihre erste Sicherung in weniger als zwei Minuten durch. Mit Retrospect kann die Wiederherstellung durch Beantwortung einiger leichter Fragen geplant werden. Wiederherstellungen lassen sich problemlos durchführen. Wenn eine Wiederherstellung erforderlich ist, ermittelt Retrospect Express automatisch die Dateien, selbst wenn Sie nicht wissen, auf welchem Medium sich die gesicherten Dateien befinden.

Duplizieren Sie Dateien und Ordner auf eine externen Festplatte durch Drücken einer Taste. Beim Duplizieren werden Informationen von der Festplatte des Computers auf eine externe Festplatte kopiert. (Bei externen Festplatten, die über eine integrierte Backup-Taste verfügen, kann die Duplizierung durch einfaches Drücken der Taste gestartet werden.) Bei der Duplizierung können die Dateien und Ordner auf der externen Festplatte schnell angezeigt, bearbeitet und über den Windows Explorer wiederhergestellt werden. Bei der Duplizierung wird zum einen Speicherplatz eingespart, da alte Sicherungsdaten auf der externen Festplatte überschrieben werden, und zum anderen Zeit, da nur die Dateien kopiert werden, die sich seit der letzten Sicherung geändert haben.

Sie können mehrere Versionen von Dateien und Ordnern sichern. Bei der umfassenden Sicherung werden ältere Versionen von Dateien und Ordnern beibehalten. So kann ein Computer in einen beliebigen Zustand vor der Beschädigung der Daten zurückgeführt werden. Bei jeder Sicherung erstellt Retrospect Express einen Wiederherstellungspunkt, der alle Informationen enthält, die ein Benutzer zum Abrufen von Dateien oder zur Wiederherstellung eines gesamten Computers (Wiederherstellung im Notfall) benötigt. Dazu zählen alle Dateien und Einstellungen des Betriebssystems, Gerätetreiber sowie Anwendungen und deren Einstellungen. Wiederherstellungspunkte lassen sich schnell erstellen, und sie gewährleisten eine 100%ige Wiederherstellung zu einem beliebigen Zeitpunkt der Sicherung. Dies übersteigt die Funktionalität anderer Softwareprodukte zur Datensicherung.

Weitere Informationen zu Dantz Retrospect Express finden Sie unter [http://www.dantz.com/en/products/win\\_express/index.dtml](http://www.dantz.com/en/products/win_express/index.dtml).

## Proactive Change Notification

Im Rahmen des Proactive Change Notification-Programms werden auf der Grundlage von Eingaben auf der Website *Subscriber's Choice* proaktiv und automatisch folgende Mails versandt:

- Eine PCN (Proactive Change Notification)-E-Mail, die Sie bis zu 60 Tage im Voraus über Änderungen der Hardware und Software der am häufigsten von Unternehmen genutzten Computer und Server informiert.
- Eine E-Mail mit Informationen, Ratschlägen und Hinweisen für Kunden, Sicherheitsmitteilungen und Treiber-Warmmeldungen für die am häufigsten von 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. Ausführlichere Informationen über das Proactive Change Notification-Programm und die Erstellung eines persönlichen Profils finden Sie unter <http://h30046.www3.hp.com/subhub.php?jumpid=go/pcn>.

## Subscriber's Choice

Subscriber's Choice ist ein Client-basierter Dienst von HP. Auf der Grundlage Ihres Profils erhalten Sie von HP individuell zugeschnittene Produkttipps, Presseartikel und/oder Meldungen/Benachrichtigungen über Treiber und Technische Kundenunterstützung. Im Rahmen der Meldungen/Benachrichtigungen über Treiber und technischen Support von Subscriber's Choice erhalten Sie E-Mails mit der Mitteilung, dass die Informationen, die Sie in Ihrem Profil als für Sie relevant angegeben haben, jetzt zum Testen und Abrufen verfügbar sind. Auf der Website unter der folgenden Adresse finden Sie ausführlichere Informationen zu Subscriber's Choice und können ein persönliches Profil erstellen: <http://h30046.www3.hp.com/subhub.php>

## Ehemalige Lösungen

Die Desktop Management Task Force (DMTF) hat den Desktop Management Interface (DMI)-Standard vor etwa zehn Jahren ins Leben gerufen. Durch notwendige Anpassungen der Standards, wie das Common Information Model (CIM), musste der DMI-Standard ersetzt werden. Durch weitere Verbesserungen bei HP Client Management Solutions, HP Systems Insight Manager und durch die Implementierung von CIM durch Microsoft, bekannt als Windows Management Instrumentation (WMI), steht der HP Insight Management Agent nicht länger auf den neuen von Unternehmen genutzten HP Desktops, Workstations und Notebooks zur Verfügung, die nach dem 1. Januar 2004 auf den Markt gekommen sind.

Insight Management (IM) Agent umfasste folgende Funktionen:

- Durch die DMI-Unterstützung konnte ein Client-System über Insight Manager 7 oder andere DMI-kompatible Management-Anwendungen verwaltet werden.
- Ein Web-Agent ermöglichte das lokale als auch das Remote-Management des Systems über einen Webbrowser.
- Warnmeldungen über den Systemzustand konnten direkt an den Benutzer oder an eine zentrale Konsole gesendet werden.

Insight Manager wurde durch die HP Systems Insight Manager-Software (HP SIM) ersetzt. HP SIM ruft Informationen zum Client-System mithilfe von WMI ab. Altiris Connector for HP Systems Insight Manager steht zur Verfügung und aktiviert die HP Client Management Solutions über die HP SIM-Konsole.

Da lokale Warnmeldungen momentan von HP Client Management Solutions nicht unterstützt werden, werden diese an der System-Management-Konsole angezeigt. Microsoft WMI ist standardmäßig in Windows 2000 und Windows XP enthalten. WMI leitet Hardwarebestands- und Warnmeldungen über das Windows-Betriebssystem an eine System-Management-Anwendung weiter.

## ROM-Flash

Das BIOS des Computers ist in einem programmierbaren Flash-ROM (ROM = Read Only Memory, Nur-Lese-Speicher) gespeichert. Wenn das BIOS aktualisiert werden muss, können Sie die neuesten BIOS-Images von der HP Seite „Treiber und Support“ unter <http://www.hp.com/support/files> herunterladen.



**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.hp.com/go/ssm>.

---

## Remote ROM Flash

Remote ROM Flash ermöglicht dem Systemadministrator, das BIOS von entfernten HP Computern direkt von der zentralen Netzwerk-Management-Konsole aus auf sichere Weise zu aktualisieren. Da der Systemadministrator diese Aufgabe per Remote-Zugriff auf mehreren Computern durchführen kann, ergibt sich dadurch ein konsistenter Einsatz und eine bessere Überwachung von BIOS-Images in HP PCs im Netzwerk. Dies führt außerdem zu höherer Produktivität und niedrigeren Total Cost of Ownership.



Der Computer muss eingeschaltet sein oder über die Remote-Aufruffunktion eingeschaltet werden, um den Remote-ROM-Flash zu nutzen.

---

Weitere Informationen zu Remote-ROM-Flash erhalten Sie in Verbindung mit HP Client Manager Software oder dem System Software Manager unter <http://h18000.www1.hp.com/im/prodinfo.html>.

## HPQFlash

HPQFlash Utility wird verwendet, um das System-BIOS auf einzelnen PCs über ein Windows-Betriebssystem lokal zu aktualisieren oder wiederherzustellen.

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.

## Boot-Block-Wiederherstellungsmodus

Der Boot-Block-Wiederherstellungsmodus ermöglicht eine Wiederherstellung des Systems im unwahrscheinlichen Fall eines ROM-Flash-Fehlers. Kommt es während des ROM-Flash zu einem Stromausfall, wird das BIOS nicht vollständig aktualisiert. Das System-BIOS wird in diesem Fall unbrauchbar. Der Boot-Block ist ein flash-geschützter Bereich des ROM-Speichers, der jedes Mal die Gültigkeit des System-BIOS-Images anhand eines Codes überprüft, wenn der Computer eingeschaltet wird.

- Wenn das BIOS-Image des Systems gültig ist, startet das System auf normale Weise.
- Ist das BIOS-Image nicht gültig, bietet das FailSafe Boot Block BIOS ausreichend Unterstützung, um Folgendes durchzuführen:
  - ❑ Suchen von BIOS-Image-Dateien auf Wechselmedien. Wird eine entsprechende BIOS-Image-Datei gefunden, wird der ROM mit dieser Datei aktualisiert.
  - ❑ Starten des Systems von einem bootfähigen Wechselmedium, mit dem automatisch Programme zur Aktualisierung des System-BIOS aufgerufen werden.

Wird ein ungültiges System-BIOS-Image gefunden, leuchtet die rote Betriebs-LED achtmal im Abstand von jeweils einer Sekunde. Gleichzeitig wird achtmal hintereinander ein akustisches Signal ausgegeben. Wenn der Teil des System-ROM mit dem Grafik-Options-ROM-Image nicht beschädigt ist, wird „Boot Block Emergency Recovery Mode“ (Boot-Block-Wiederherstellungsmodus) auf dem Bildschirm angezeigt.

So stellen Sie das System wieder her, nachdem es in den Boot-Block-Wiederherstellungsmodus geschaltet hat:

1. Schalten Sie den Computer aus.
2. Legen Sie eine Diskette oder eine CD ein, oder schließen Sie ein USB-Flash-Laufwerk an, auf dem die gewünschte BIOS-Image-Datei im Stammverzeichnis enthalten ist.  
Hinweis: Das Medium muss im Dateisystem FAT12, FAT16 oder FAT32 formatiert sein.

3. Schalten Sie den Computer ein.

Wurde keine geeignete BIOS-Image-Datei gefunden, startet das Failsafe Boot Block BIOS das System von einem bootfähigen Gerät aus. Wird kein bootfähiges Gerät erkannt, werden Sie aufgefordert, ein Medium mit einer BIOS-Image-Datei oder einem Programm zur BIOS-Aktualisierung einzulegen.

Wenn der ROM erfolgreich umprogrammiert wurde, wird der Computer automatisch ausgeschaltet.

4. Nehmen Sie das für die Aktualisierung des BIOS verwendete Wechselmedium heraus.
5. Starten Sie den Computer anschließend neu.

## Replizieren des Setup

Das folgende 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.



Bei beiden Verfahren ist ein Diskettenlaufwerk oder ein unterstütztes USB-Flash-Laufwerk, wie z. B. ein HP USB Memory Key, erforderlich.

---

---

## Kopieren auf einen einzelnen Computer

---



**ACHTUNG:** Eine Setup-Konfiguration ist modellspezifisch. Das Dateisystem kann beschädigt werden, wenn Ursprungs- und Zielcomputer nicht das gleiche Modell haben. Kopieren Sie beispielsweise nicht die Setup-Konfiguration eines dc7xxx PC auf einen dx7xxx PC.

---

1. Wählen Sie die Setup-Konfiguration aus, die kopiert werden soll. Schalten Sie den Computer aus. Klicken Sie unter Windows auf **Start > Beenden > Herunterfahren**.
  2. Wenn Sie ein USB-Flash-Laufwerk verwenden, schließen Sie es jetzt an.
  3. Schalten Sie den Computer ein.
  4. Drücken Sie sofort nach dem Einschalten des Computers, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10**, um Computer Setup aufzurufen. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.
- 



Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten. Halten Sie dann, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10** gedrückt, um das Dienstprogramm aufzurufen.

---

5. Wenn Sie eine Diskette verwenden, legen Sie sie jetzt ein.
6. Klicken Sie auf die Befehlsfolge **File > Replicated Setup > Save to Removable Media** (Datei > Repliziertes Setup > Auf Wechsellaufwerk speichern). Folgen Sie den Anleitungen auf dem Bildschirm, um die Konfigurationsdiskette oder das USB-Flash-Laufwerk zu erstellen.
7. Schalten Sie den Computer aus, der konfiguriert werden soll. Legen Sie dann die Konfigurationsdiskette ein, oder schließen Sie das USB-Flash-Laufwerk an.
8. Schalten Sie den zu konfigurierenden Computer ein.
9. Drücken Sie sofort nach dem Einschalten des Computers, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10**, um Computer Setup aufzurufen. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.

10. Klicken Sie auf die Befehlsfolge **File > Replicated Setup > Restore from Removable Media** (Datei > Repliziertes Setup > Von Wechsellaufwerk wiederherstellen).
11. Starten Sie den Computer neu, wenn die Konfiguration abgeschlossen ist.

## Kopieren auf mehrere Computer

---



**ACHTUNG:** Eine Setup-Konfiguration ist modellspezifisch. Das Dateisystem kann beschädigt werden, wenn Ursprungs- und Zielcomputer nicht das gleiche Modell haben. Kopieren Sie beispielsweise nicht die Setup-Konfiguration eines dc7xxx PC auf einen dx7xxx PC.

---

Bei dieser Methode dauert es etwas länger, die Konfigurationsdiskette oder das USB-Flash-Laufwerk vorzubereiten. Das Kopieren der Konfiguration auf die Zielcomputer dagegen geht wesentlich schneller.

---



Für dieses Verfahren ist eine bootfähige Diskette erforderlich, oder es muss ein bootfähiges USB-Flash-Laufwerk erstellt werden. Wenn unter Windows XP keine bootfähige Diskette erstellt werden kann, wenden Sie statt dessen das Verfahren zum Kopieren auf einen einzelnen Computer an (siehe „[Kopieren auf einen einzelnen Computer](#)“ auf Seite 17).

---

1. Erstellen Sie eine bootfähige Diskette oder ein bootfähiges USB-Flash-Laufwerk. Informationen hierzu finden Sie unter „[Unterstütztes USB-Flash-Laufwerk](#)“ auf Seite 20 oder „[Nicht unterstütztes USB-Flash-Laufwerk](#)“ auf Seite 22.
- 



**ACHTUNG:** Nicht alle Computer können von einem USB-Flash-Laufwerk aus gestartet werden. Wenn in der standardmäßigen Startreihenfolge in Computer Setup (F10) das USB-Laufwerk vor dem Festplattenlaufwerk aufgeführt ist, kann der Computer von einem USB-Flash-Laufwerk aus gestartet werden. Andernfalls muss eine bootfähige Diskette verwendet werden.

---

2. Wählen Sie die Setup-Konfiguration aus, die kopiert werden soll. Schalten Sie den Computer aus. Klicken Sie unter Windows auf **Start > Beenden > Herunterfahren**.
3. Wenn Sie ein USB-Flash-Laufwerk verwenden, schließen Sie es jetzt an.

4. Schalten Sie den Computer ein.
5. Drücken Sie sofort nach dem Einschalten des Computers, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10**, um Computer Setup aufzurufen. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



---

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten. Halten Sie dann, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10** gedrückt, um das Dienstprogramm aufzurufen.

---

6. Wenn Sie eine Diskette verwenden, legen Sie sie jetzt ein.
7. Klicken Sie auf die Befehlsfolge **File > Replicated Setup > Save to Removable Media** (Datei > Repliziertes Setup > Auf Wechsellaufwerk speichern). Folgen Sie den Anleitungen auf dem Bildschirm, um die Konfigurationsdiskette oder das USB-Flash-Laufwerk zu erstellen.
8. Laden Sie ein BIOS-Dienstprogramm zum Replizieren des Setup herunter (repset.exe), und kopieren Sie es auf die Konfigurationsdiskette oder das USB-Flash-Laufwerk. Um dieses Programm herunterzuladen, rufen Sie die Website <http://www.hp.com/support> auf und geben die Modellnummer des Computers ein.
9. Erstellen Sie auf der Konfigurationsdiskette oder dem USB-Flash-Laufwerk eine autoexec.bat-Datei, die folgenden Befehl enthält:  
**repset.exe**
10. Schalten Sie den zu konfigurierenden Computer aus. Legen Sie die Konfigurationsdiskette ein, oder schließen Sie das USB-Flash-Laufwerk an. Schalten Sie dann den Computer wieder ein. Das Konfigurationsdienstprogramm wird automatisch ausgeführt.
11. Starten Sie den Computer neu, wenn die Konfiguration abgeschlossen ist.

## Erstellen eines bootfähigen Geräts

### Unterstütztes USB-Flash-Laufwerk

Unterstützte Geräte verfügen über ein vorinstalliertes Image, das die Bootfähigkeit unterstützt. Auf allen HP oder Compaq Geräten sowie auf den meisten USB-Flash-Laufwerken ist dieses Image vorinstalliert. Wenn das verwendete USB-Flash-Laufwerk kein solches Image hat, verwenden Sie das weiter unten in diesem Abschnitt beschriebene Verfahren (siehe „Nicht unterstütztes USB-Flash-Laufwerk“ auf Seite 22).

Um ein bootfähiges USB-Flash-Laufwerk zu erstellen, benötigen Sie:

- ein unterstütztes USB-Flash-Laufwerk
- eine bootfähige DOS-Diskette mit FDISK- und SYS-Programmen. (Wenn SYS nicht verfügbar ist, kann FORMAT verwendet werden. Allerdings gehen dann alle auf dem USB-Flash-Laufwerk vorhandenen Dateien verloren.)
- einen Computer, der über ein USB-Flash-Laufwerk gestartet werden kann.



**ACHTUNG:** Einige ältere Modelle lassen sich unter Umständen nicht von einem USB-Flash-Laufwerk starten. Wenn in der standardmäßigen Startreihenfolge in Computer Setup (F10) das USB-Laufwerk vor dem Festplattenlaufwerk aufgeführt ist, kann der Computer von einem USB-Flash-Laufwerk aus gestartet werden. Andernfalls muss eine bootfähige Diskette verwendet werden.

---

1. Schalten Sie den Computer aus.
2. Schließen Sie das USB-Flash-Laufwerk an einen der USB-Ports des Computers an, und entfernen Sie alle anderen USB-Speichergeräte, mit Ausnahme von USB-Diskettenlaufwerken.
3. Legen Sie eine bootfähige DOS-Diskette mit FDISK.COM und mit entweder SYS.COM oder FORMAT.COM in das Diskettenlaufwerk ein. Schalten Sie dann den Computer ein, um von der DOS-Diskette zu starten.
4. Führen Sie FDISK aus, indem Sie an der Eingabeaufforderung A:\ **FDISK** eingeben und die Eingabetaste drücken. Klicken Sie auf **Yes (Y)**, um die Unterstützung für große Laufwerke zu aktivieren.

5. Geben Sie **Choice [5]** ein, um die Laufwerke im System anzuzeigen. Das USB-Flash-Laufwerk ist das Laufwerk, das weitgehend der Größe eines der aufgelisteten Laufwerke entspricht. Es ist in der Regel das letzte Laufwerk in der Liste. Notieren Sie den Laufwerksbuchstaben.

USB-Flash-Laufwerk: \_\_\_\_\_



**ACHTUNG:** Wenn kein Laufwerk dem USB-Flash-Laufwerk entspricht, fahren Sie nicht fort. Daten können verloren gehen. Überprüfen Sie alle USB-Ports auf zusätzliche Speichergeräte. Entfernen Sie diese zusätzlichen Speichergeräte, starten Sie den Computer neu, und fahren Sie mit Schritt 4 fort. Wenn keine zusätzlichen Speichergeräte gefunden werden, unterstützt das System entweder das USB-Flash-Laufwerk nicht, oder das USB-Flash-Laufwerk ist defekt. Versuchen Sie NICHT weiter, das USB-Flash-Laufwerk bootfähig zu machen.

6. Verlassen Sie FDISK, indem Sie die **Esc-Taste** drücken, und kehren Sie zur Eingabeaufforderung A:\ zurück.
7. Wenn Ihre bootfähige DOS-Diskette SYS.COM enthält, gehen Sie zu Schritt 8. Andernfalls gehen Sie zu Schritt 9.
8. Geben Sie an der Eingabeaufforderung A:\ **SYS x:** ein, wobei x für den weiter oben notierten Laufwerksbuchstaben steht.



**ACHTUNG:** Vergewissern Sie sich, dass Sie den richtigen Laufwerksbuchstaben für das USB-Flash-Laufwerk eingegeben haben.

Nachdem die Systemdateien übertragen wurden, kehrt SYS wieder zur Eingabeaufforderung A:\ zurück. Gehen Sie zu Schritt 13.

9. Kopieren Sie alle Dateien, die Sie behalten möchten, von dem USB-Flash-Laufwerk in ein temporäres Verzeichnis auf einem anderen Laufwerk (z. B. das interne Festplattenlaufwerk).
10. Geben Sie an der Eingabeaufforderung A:\ **FORMAT /S X:** ein, wobei X für den weiter oben notierten Laufwerksbuchstaben steht.



**ACHTUNG:** Vergewissern Sie sich, dass Sie den richtigen Laufwerksbuchstaben für das USB-Flash-Laufwerk eingegeben haben.

FORMAT zeigt eine oder mehrere Warnmeldungen an, und fragt Sie jedes Mal, ob Sie fortfahren möchten. Geben Sie jedes Mal **Y** (Ja) ein. FORMAT formatiert das USB-Flash-Laufwerk, fügt die Systemdateien hinzu, und fordert Sie auf, einen Namen für den Datenträger anzugeben.

11. Drücken Sie die **Eingabetaste**, wenn Sie keinen Namen eingeben möchten, oder geben Sie einen Namen ein.
12. Kopieren Sie alle in Schritt 9 gesicherten Dateien wieder auf das USB-Flash-Laufwerk.
13. Nehmen Sie die Diskette heraus, und starten Sie den Computer neu. Der Computer startet mit dem USB-Flash-Laufwerk als Laufwerk C.



---

Die standardmäßige Startreihenfolge variiert von Computer zu Computer. Sie kann in Computer Setup geändert werden.

Wenn Sie eine DOS-Version von Windows 9x verwenden, wird kurz ein Bildschirm mit dem Windows-Logo angezeigt. Wenn dieser Bildschirm nicht angezeigt werden soll, fügen Sie dem Root-Verzeichnis des USB-Flash-Laufwerks eine Datei mit Nulllänge namens LOGO.SYS hinzu.

---

Gehen Sie wieder zu „[Kopieren auf mehrere Computer](#)“ auf Seite 18.

## **Nicht unterstütztes USB-Flash-Laufwerk**

Um ein bootfähiges USB-Flash-Laufwerk zu erstellen, benötigen Sie:

- ein USB-Flash-Laufwerk.
- eine bootfähige DOS-Diskette mit FDISK- und SYS-Programmen. (Wenn SYS nicht verfügbar ist, kann FORMAT verwendet werden. Allerdings gehen dann alle auf dem USB-Flash-Laufwerk vorhandenen Dateien verloren.)
- einen Computer, der über ein USB-Flash-Laufwerk gestartet werden kann.



**ACHTUNG:** Einige ältere Modelle lassen sich unter Umständen nicht von einem USB-Flash-Laufwerk starten. Wenn in der standardmäßigen Startreihenfolge in Computer Setup (F10) das USB-Laufwerk vor dem Festplattenlaufwerk aufgeführt ist, kann der Computer von einem USB-Flash-Laufwerk aus gestartet werden. Andernfalls muss eine bootfähige Diskette verwendet werden.

1. Wenn sich im System PCI-Karten befinden, an die SCSI-, ATA RAID- oder SATA-Laufwerke angeschlossen sind, schalten Sie den Computer aus, und ziehen Sie das Netzkabel.



**ACHTUNG:** Das Netzkabel MUSS herausgezogen werden.

2. Öffnen Sie den Computer, und nehmen Sie die PCI-Karten heraus.
3. Schließen Sie das USB-Flash-Laufwerk an einen der USB-Ports des Computers an, und entfernen Sie alle anderen USB-Speichergeräte, mit Ausnahme von USB-Diskettenlaufwerken. Schließen Sie die Gehäuseabdeckung.
4. Schließen Sie das Netzkabel an die Stromversorgung an, und schalten Sie den Computer ein.
5. Drücken Sie sofort nach dem Einschalten des Computers, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10**, um Computer Setup aufzurufen. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten. Halten Sie dann, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10** gedrückt, um das Dienstprogramm aufzurufen.

6. Deaktivieren Sie die PATA- und SATA-Controller unter **Advanced > PCI Devices** (Erweitert > PCI-Geräte). Notieren Sie beim Deaktivieren des SATA-Controllers die zugeordnete IRQ-Adresse. Sie müssen die IRQ-Adresse später wieder zuordnen. Beenden Sie Setup, und bestätigen Sie die Änderungen.

SATA-IRQ: \_\_\_\_\_

7. Legen Sie eine bootfähige DOS-Diskette mit `FDISK.COM` und mit entweder `SYS.COM` oder `FORMAT.COM` in das Diskettenlaufwerk ein. Schalten Sie dann den Computer ein, um von der DOS-Diskette zu starten.
8. Führen Sie `FDISK` aus, und löschen Sie alle bestehenden Partitionen auf dem USB-Flash-Laufwerk. Erstellen Sie eine neue Partition, und kennzeichnen Sie sie als aktiv. Verlassen Sie `FDISK`, indem Sie die **Esc-Taste** drücken.
9. Wenn das System beim Beenden von `FDISK` nicht automatisch neu startet, drücken Sie die Tastenkombination **Strg+Alt+Entf**, um die DOS-Diskette zu starten.
10. Geben Sie an der Eingabeaufforderung `A:\` **FORMAT C: /S** ein, und drücken Sie die **Eingabetaste**. `FORMAT` formatiert das USB-Flash-Laufwerk, fügt die Systemdateien hinzu, und fordert Sie auf, einen Namen für den Datenträger einzugeben.
11. Drücken Sie die **Eingabetaste**, wenn Sie keinen Namen eingeben möchten, oder geben Sie einen Namen ein.
12. Schalten Sie den Computer aus, und ziehen Sie das Netzkabel. Öffnen Sie den Computer, und installieren Sie wieder alle zuvor entfernten PCI-Karten. Schließen Sie die Gehäuseabdeckung.
13. Schließen Sie das Netzkabel an, nehmen Sie die Diskette heraus, und schalten Sie den Computer ein.
14. Drücken Sie sofort nach dem Einschalten des Computers, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10**, um Computer Setup aufzurufen. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.
15. Aktivieren Sie erneut die PATA- und SATA-Controller unter **Advanced > PCI Devices** (Erweitert > PCI-Geräte), die Sie in Schritt 6 deaktiviert hatten. Ordnen Sie dem SATA-Controller wieder die ursprüngliche IRQ-Adresse zu.
16. Speichern Sie die Änderungen und beenden Sie die Anwendung. Der Computer startet mit dem USB-Flash-Laufwerk als Laufwerk C.



Die standardmäßige Startreihenfolge variiert von Computer zu Computer. Sie kann in Computer Setup geändert werden. Anleitungen finden Sie im *Computer Setup (F10) Utility Handbuch* auf der CD *Documentation and Diagnostics*.

Wenn Sie eine DOS-Version von Windows 9x verwenden, wird kurz ein Bildschirm mit dem Windows-Logo angezeigt. Wenn dieser Bildschirm nicht angezeigt werden soll, fügen Sie dem Root-Verzeichnis des USB-Flash-Laufwerks eine Datei mit Nulllänge namens LOGO.SYS hinzu.

Gehen Sie wieder zu „[Kopieren auf mehrere Computer](#)“ auf Seite 18.

## Dual-State-Netzschalter

Wenn ACPI (Advanced Configuration and Power Interface) aktiviert ist, kann der Netzschalter die Funktion eines Ein-/Aus-Schalters oder eines Standby-Schalters haben. Im Standby-Modus wird die Stromzufuhr nicht vollständig unterbrochen, sondern der Computer schaltet auf geringen Stromverbrauch um. Auf diese Weise können Sie schnell in den Energiesparmodus schalten, ohne die Anwendungen schließen zu müssen, und Sie können ohne Datenverlust schnell wieder in den vorherigen Betriebszustand zurückkehren.

So ändern Sie die Konfiguration des Netzschalters:

1. Klicken Sie mit der linken Maustaste auf **Start**, und wählen Sie **Systemsteuerung > Energieoptionen**.
2. Öffnen Sie unter **Eigenschaften von Energieoptionen** die Registerkarte **Erweitert**.
3. Wählen Sie im Abschnitt **Netzschalter** die Option **Standby**.

Wenn Sie den Netzschalter als Standby-Taste konfiguriert haben, wird das System durch Drücken des Schalters in einen Zustand mit sehr geringem Stromverbrauch geschaltet (Standby-Modus). Durch erneutes Drücken der Standby-Taste schalten Sie aus dem Standby-Modus wieder auf Normalbetrieb um. Wenn Sie die Stromzufuhr ganz unterbrechen möchten, 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 andernfalls die Gefahr besteht, dass die Festplatte beschädigt wird oder Daten verloren gehen.

## HP Website

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 aktuellsten 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 und entsprechen den folgenden Industriestandards:

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

## Bestandsüberwachung und Sicherheit

Die auf dem Computer vorinstallierten Bestandsüberwachungsfunktionen stellen Ihnen wichtige Daten zur Bestandsüberwachung bereit, die über HP Systems Insight Manager, HP Client Manager oder andere Systemverwaltungsanwendungen verwaltet werden können. Die nahtlose automatische Integration dieser 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. HP Embedded Security for ProtectTools verhindert den unbefugten Zugriff auf Daten, überprüft die Systemintegrität und authentifiziert Drittbenedutzer, die versuchen, auf das System zuzugreifen. (Weitere Informationen finden Sie im *HP ProtectTools Security Manager Handbuch* unter [www.hp.com](http://www.hp.com).) Sicherheitsfunktionen wie HP Embedded Security for ProtectTools, der Smart Cover Sensor und das Smart Cover Lock, die für einige Modelle verfügbar sind, schützen vor unberechtigtem 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 System-Management-Programme weitergeleitet werden, um darüber zu informieren, dass sich jemand unerlaubten Zugang zu den internen Komponenten des Computers verschafft.



---

HP Embedded Security for ProtectTools, der Smart Cover Sensor und das Smart Cover Lock sind bei einigen Modellen optional erhältlich.

---

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

- Lokal: Computer Setup. Weitere Informationen und Anleitungen zur Verwendung von Computer Setup finden Sie im *Computer Setup (F10) Utility Handbuch* auf der CD *Documentation and Diagnostics*, die im Lieferumfang des Computers enthalten ist.
- Remote: HP Client Manager oder System Software Manager. Diese Software ermöglicht die sichere, einheitliche Implementierung und Steuerung von Sicherheitseinstellungen über ein einfaches Befehlszeilen-Dienstprogramm.

Die folgende Tabelle und die folgenden Abschnitte beziehen sich auf das lokale Verwalten von Sicherheitsfunktionen des Computers mithilfe von Computer Setup.

## Überblick über die Sicherheitsfunktionen

Option	Beschreibung
<b>Setup Password</b>	<p>Ermöglicht das Einrichten und Aktivieren des Setup-Kennworts (Administrator-Kennwort).</p> <p> Wenn das Setup-Kennwort eingerichtet wurde, ist seine Eingabe erforderlich, wenn die Optionen für Computer Setup geändert und der ROM-Speicher aktualisiert oder Änderungen an bestimmten Plug-and-Play-Einstellungen unter Windows vorgenommen werden sollen.</p> <p>Weitere Informationen finden Sie im <i>Fehlerbeseitigungs-Handbuch</i> auf der CD <i>Documentation and Diagnostics</i>.</p>
<b>Power-On Password</b> (Kennwort für den Systemstart)	<p>Zum Einrichten und Aktivieren des Kennworts für den Systemstart.</p> <p>Weitere Informationen finden Sie im <i>Fehlerbeseitigungs-Handbuch</i> auf der CD <i>Documentation and Diagnostics</i>.</p>
<b>Password Options</b> (Kennwortoptionen) (Diese Option wird nur angezeigt, wenn ein Kennwort für den Systemstart festgelegt wurde.)	<p>Zur Angabe, ob das Kennwort für den Warmstart (<b>STRG+ALT+ENTF</b>) erforderlich sein soll.</p> <p>Weitere Informationen finden Sie im <i>Computer Setup (F10) Utility Handbuch</i> auf der CD <i>Documentation and Diagnostics</i>.</p>
<b>Pre-Boot Authorization</b> (PBA)	<p>Zum Aktivieren/Deaktivieren der Smart Card, die anstelle des Kennworts für den Systemstart verwendet wird.</p>
	<p> Weitere Informationen zur Verwendung von Computer Setup finden Sie im <i>Computer Setup (F10) Utility Handbuch</i> auf der CD <i>Documentation and Diagnostics</i>.</p> <p>Die Unterstützung von Sicherheitsfunktionen kann je nach Computer-Konfiguration unterschiedlich sein.</p>

---

## Überblick über die Sicherheitsfunktionen (Fortsetzung)

---

Option	Beschreibung
<b>Smart Cover</b>	<p>Ermöglicht Ihnen folgende Einstellungen:</p> <ul style="list-style-type: none"> <li>• Aktivieren und Deaktivieren des Smart Cover Lock.</li> <li>• Aktivieren/Deaktivieren des Cover Removal Sensor.</li> </ul> <p> Mit <i>Notify User</i> (Benutzer benachrichtigen) wird der Benutzer benachrichtigt, sobald der Sensor erkannt hat, dass die Abdeckung entfernt wurde. Mit <i>Setup Password</i> (Setup-Kennwort) wird festgelegt, dass das Setup-Kennwort zum Starten des Computers eingegeben werden muss, wenn der Sensor erkannt hat, dass die Abdeckung entfernt wurde.</p> <p>Diese Funktion wird nur bei einigen Modellen unterstützt. Weitere Informationen finden Sie im <i>Computer Setup (F10) Utility Handbuch</i> auf der CD <i>Documentation and Diagnostics</i>.</p>
<b>Embedded Security</b>	<p>Ermöglicht Ihnen folgende Einstellungen:</p> <ul style="list-style-type: none"> <li>• Aktivieren/Deaktivieren der Embedded Security-Funktion.</li> <li>• Zurücksetzen der Funktion auf die voreingestellten Standardeinstellungen.</li> </ul> <p>Diese Funktion wird nur bei einigen Modellen unterstützt. Weitere Informationen finden Sie im <i>HP ProtectTools Security Manager Handbuch</i> unter <a href="http://www.hp.com">www.hp.com</a>.</p>
<b>Device Security</b> (Gerätesicherheit)	<p>Aktiviert/Deaktiviert serielle und parallele Anschlüsse, USB-Anschlüsse auf der Vorderseite, das Audiosystem, Netzwerk-Controller (bei einigen Modellen), MultiBay Geräte (bei einigen Modellen) und SCSI-Controller (bei einigen Modellen).</p>
<p> Weitere Informationen zur Verwendung von Computer Setup finden Sie im <i>Computer Setup (F10) Utility Handbuch</i> auf der CD <i>Documentation and Diagnostics</i>.</p> <p>Die Unterstützung von Sicherheitsfunktionen kann je nach Computer-Konfiguration unterschiedlich sein.</p>	

---

## Überblick über die Sicherheitsfunktionen (Fortsetzung)

---

Option	Beschreibung
<b>Network Service Boot</b> (Starten über Netzwerk)	Aktiviert/deaktiviert die Funktion zum Starten von einem Betriebssystem, das auf einem Netzwerksystem installiert ist. (Diese Funktion steht nur für NIC-Modelle zur Verfügung. Der Netzwerk-Controller muss sich auf dem PCI-Bus befinden oder auf der Systemplatine integriert sein.)
<b>System IDs</b> (System-IDs)	Folgende Einstellungen können vorgenommen werden: <ul style="list-style-type: none"> <li>• Bestandskennung (18-Byte-Kennung) und Eigentümerkennung (80-Byte-Kennung, die während des POST angezeigt wird).</li> </ul> Weitere Informationen finden Sie im <i>Computer Setup (F10) Utility Handbuch</i> auf der CD <i>Documentation and Diagnostics</i> . <ul style="list-style-type: none"> <li>• 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 zur eindeutigen Identifizierung des Systems verwendet.)</li> </ul> Landesspezifische Tastatureinstellungen (z. B. Englisch oder Deutsch) für die Eingabe der System-ID.
	Weitere Informationen zur Verwendung von Computer Setup finden Sie im <i>Computer Setup (F10) Utility Handbuch</i> auf der CD <i>Documentation and Diagnostics</i> . Die Unterstützung von Sicherheitsfunktionen kann je nach Computer-Konfiguration unterschiedlich sein.

---

---

## Überblick über die Sicherheitsfunktionen (Fortsetzung)

---

Option	Beschreibung
<b>DriveLock</b> (einige Modelle)	<p>Ermöglicht die Zuweisung oder Änderung eines Master- oder Benutzerkennworts für ATA-Festplatten. Wenn diese Funktion aktiviert ist, wird der Benutzer dazu aufgefordert, während des POST eines der DriveLock-Kennwörter einzugeben. Wird keines erfolgreich eingegeben, kann solange nicht auf die Festplatte zugegriffen werden, bis eines der Kennwörter richtig während eines Kaltstarts eingegeben wird.</p> <p> Diese Option wird nur angezeigt, wenn mindestens ein ATA-Laufwerk, das den ATA-Sicherheitsbefehlssatz unterstützt, mit dem System verbunden ist.</p> <p>Weitere Informationen finden Sie im <i>Computer Setup (F10) Utility Handbuch</i> auf der CD <i>Documentation and Diagnostics</i>.</p>
	<p>Weitere Informationen zur Verwendung von Computer Setup finden Sie im <i>Computer Setup (F10) Utility Handbuch</i> auf der CD <i>Documentation and Diagnostics</i>.</p> <p>Die Unterstützung von Sicherheitsfunktionen kann je nach Computer-Konfiguration unterschiedlich sein.</p>

---

## Kennwort-Schutz

Das Kennwort für den Systemstart verhindert die unbefugte Verwendung des Computers, indem für den Zugriff auf Anwendungen oder Daten bei jedem Einschalten oder Neustart des Computers die Eingabe eines Kennworts erforderlich ist. Das Setup-Kennwort verhindert insbesondere den unbefugten Zugriff auf Computer Setup und kann auch verwendet werden, um das Kennwort für den Systemstart zu übergehen. Der Zugriff auf den Computer wird also gewährt, wenn bei der Eingabeaufforderung das Setup-Kennwort anstelle des Kennworts für den Systemstart eingegeben wird.

Es kann auch ein für das gesamte Netzwerk gültiges Kennwort 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 das System mit Embedded Security ausgestattet ist, finden Sie weitere Informationen im *HP ProtectTools Security Manager Handbuch* unter [www.hp.com](http://www.hp.com). 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 unter Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie sofort nach dem Einschalten des Computers, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10**, um Computer Setup aufzurufen. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten. Halten Sie dann, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10** gedrückt, um das Dienstprogramm aufzurufen.

---

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

## Einrichten des Kennworts für den Systemstart über Computer Setup

Wenn ein Kennwort für den Systemstart über Computer Setup festgelegt wird, kann auf den Computer erst zugegriffen werden, nachdem das Kennwort eingegeben wurde. Wenn ein Kennwort für den Systemstart festgelegt wird, zeigt Computer Setup im Menü **Security** (Sicherheit) Kennwortoptionen an. Dazu gehört die Option **Password Prompt on Warm Boot** (Aufforderung zur Eingabe des Kennworts beim Warmstart). 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 unter Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie sofort nach dem Einschalten des Computers, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10**, um Computer Setup aufzurufen. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten. Halten Sie dann, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10** gedrückt, um das Dienstprogramm aufzurufen.

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

## Eingabe des 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 dann die **Eingabetaste**.



Nehmen Sie die Eingabe sorgfältig vor. Die eingegebenen Zeichen werden aus Sicherheitsgründen nicht auf dem Bildschirm 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.

## Eingabe eines Setup-Kennworts

Wenn das System mit Embedded Security ausgestattet ist, finden Sie weitere Informationen im *HP ProtectTools Embedded Security Handbuch* unter [www.hp.com](http://www.hp.com).

Wenn für den Computer ein Setup-Kennwort eingerichtet wurde, werden Sie bei jeder Ausführung von Computer Setup zur Eingabe dieses Kennworts aufgefordert.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie unter Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie sofort nach dem Einschalten des Computers, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10**, um Computer Setup aufzurufen. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



---

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten. Halten Sie dann, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10** gedrückt, um das Dienstprogramm aufzurufen.

---

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



---

Nehmen Sie die Eingabe sorgfältig vor. Die eingegebenen Zeichen werden aus Sicherheitsgründen nicht auf dem Bildschirm 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

Wenn das System mit Embedded Security ausgestattet ist, finden Sie weitere Informationen im *HP ProtectTools Embedded Security Handbuch* unter [www.hp.com](http://www.hp.com).

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie unter Windows auf **Start > Beenden > Neu starten**.
2. Um das Kennwort für den Systemstart zu ändern, fahren Sie mit Schritt 3 fort.

Um das Setup-Kennwort zu ändern, drücken Sie sofort nach dem Einschalten des Computers, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10**, wodurch Computer Setup aufgerufen wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten. Halten Sie dann, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10** gedrückt, um das Dienstprogramm aufzurufen.

3. Wenn das Schlüsselsymbol angezeigt wird, geben Sie Folgendes ein: das aktuelle Kennwort, einen Schrägstrich (/) oder ein anderes Begrenzungszeichen, das neue Kennwort, einen weiteren Schrägstrich (/) oder ein anderes Begrenzungszeichen und ein zweites Mal das neue Kennwort. Beispiel:

**aktuelles Kennwort/neues Kennwort/neues Kennwort**



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

4. Drücken Sie die **Eingabetaste**.

Das neue Kennwort ist ab dem nächsten Start des Computers gültig.



Weitere Informationen zu Begrenzungszeichen finden Sie im Abschnitt „[Begrenzungszeichen auf landesspezifischen Tastaturen](#)“ auf Seite 37. Sie können das Kennwort für den Systemstart und das Setup-Kennwort auch mithilfe der Sicherheitsoptionen in Computer Setup ändern.

## Löschen des Kennworts für den Systemstart oder des Setup-Kennworts

Wenn das System mit Embedded Security ausgestattet ist, finden Sie weitere Informationen im *HP ProtectTools Embedded Security Handbuch* unter [www.hp.com](http://www.hp.com).

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie unter Windows auf **Start > Beenden > Neu starten**.
2. Um das Kennwort für den Systemstart zu löschen, fahren Sie mit Schritt 3 fort.

Um das Setup-Kennwort zu löschen, drücken Sie sofort nach dem Einschalten des Computers, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10**, wodurch Computer Setup aufgerufen wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten. Halten Sie dann, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10** gedrückt, um das Dienstprogramm aufzurufen.

3. Wenn das Schlüsselsymbol angezeigt wird, geben Sie das aktuelle Kennwort, gefolgt von einem Schrägstrich (/) oder einem anderen Begrenzungszeichen ein. Beispiel:  
**aktuelles Kennwort/**
4. Drücken Sie die **Eingabetaste**.



Weitere Informationen zu Begrenzungszeichen finden Sie im Abschnitt „[Begrenzungszeichen auf landesspezifischen Tastaturen](#)“. Sie können das Kennwort für den Systemstart und das Setup-Kennwort auch mithilfe der Sicherheitsoptionen in Computer Setup ändern.

---

## 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, 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	-	Korea	/	Taiwanesisch	/
Dänisch	-	Lateinamerikanisch (Spanisch/ Portugiesisch)	-	Thailändisch	/
Französisch	!	Norwegisch	-	Türkisch	.
Kanadisches Französisch	é	Polnisch	-	Britisches Englisch	/
Deutsch	-	Portugiesisch	-	Amerikanisches Englisch	/

\*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* auf der CD *Documentation and Diagnostics*.

Wenn das System mit Embedded Security ausgestattet ist, finden Sie weitere Informationen im *HP ProtectTools Security Manager Handbuch* unter [www.hp.com](http://www.hp.com).

## DriveLock

**DriveLock** ist eine Sicherheitsfunktion, die den unbefugten Zugriff auf Daten von ATA-Festplatten verhindert. DriveLock wurde als Erweiterung von Computer Setup implementiert. Die Funktion ist nur verfügbar, wenn Festplatten erkannt werden, die den ATA-Sicherheitsbefehlssatz unterstützen. DriveLock richtet sich an Kunden von HP, deren oberste Priorität die Sicherheit ihrer Daten ist. Bei diesen Kunden stehen die Kosten für eine Festplatte und der Verlust der darauf gespeicherten Daten in keinem Verhältnis zu dem Schaden, der bei unberechtigtem Zugriff darauf entstehen kann. Damit dieses hohe Sicherheitsniveau nicht zu allzu großen Problemen führt, wenn ein Kennwort vergessen wird, wird bei der Implementierung von DriveLock durch HP ein Sicherheitssystem mit zwei Kennwörtern verwendet. Dabei sollte ein Kennwort vom Systemadministrator festgelegt und verwendet werden und das zweite vom jeweiligen Benutzer. 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. Falls beide Kennwörter für DriveLock vergessen werden, bleibt der Zugriff auf die Festplatte dauerhaft gesperrt. Dies stellt für Benutzer, die nicht dem obigen Kundenprofil entsprechen, unter Umständen ein inakzeptables Risiko dar. Für Benutzer, die diesem Profil entsprechen, bedeutet es jedoch im Hinblick auf die auf der Festplatte gespeicherten Daten ein Risiko, das hingenommen werden kann.

## Verwenden von DriveLock

**DriveLock** wird als Option im Menü **Security** (Sicherheit) von Computer Setup angezeigt. 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 empfiehlt grundsätzlich die Festlegung eines Masterkennworts durch den Administrator, unabhängig davon, ob DriveLock aktiviert wird. Dadurch hat der Administrator die Möglichkeit, DriveLock-Einstellungen zu ändern, wenn das Laufwerk einmal gesperrt sein sollte. Wenn das Masterkennwort festgelegt ist, 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. Es stehen zwei Versuche zur richtigen Kennworteingabe frei. Wenn zweimal das falsche Kennwort eingegeben wird, wird der POST zwar fortgesetzt, das Festplattenlaufwerk bleibt aber weiterhin gesperrt.

## **Anwendungen von DriveLock**

Am besten ist die DriveLock-Sicherheitsfunktion für Firmenumgebungen geeignet. Der Systemadministrator hat die Aufgabe, die Festplatte zu konfigurieren, was das Festlegen des DriveLock-Masterkennworts einschließt. 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, auch eine Firmenrichtlinie zur Einrichtung und Verwaltung von Masterkennwörtern zu erstellen. 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. Wenn kein Masterkennwort festgelegt wird, könnte es außerdem geschehen, dass Systemadministratoren selbst auf eine gesperrte Festplatte treffen und 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 potenzielle Verlust einer Festplatte aufgrund von zwei vergessenen Kennwörtern größer als der mit DriveLock geschützte Wert. 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 verhindern, dass Benutzer DriveLock aktivieren.

## Smart Cover Sensor

Der Smart Cover Sensor (nur bei einigen Modellen) ist eine Kombination aus Hardware- und Softwaretechnologie und 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 Sensor

Stufe	Einstellung	Beschreibung
Stufe 0	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 angezeigt, dass die Gehäuse- bzw. die Seitenabdeckung entfernt wurde.
Stufe 2	Setup Password (Setup-Kennwort)	Wenn der Computer neu gestartet wird, wird auf dem Bildschirm eine Meldung angezeigt, dass die Gehäuse- bzw. die Seitenabdeckung entfernt wurde. Sie müssen das Setup-Kennwort eingeben, um fortfahren zu können.



Diese Einstellungen können mithilfe von Computer Setup geändert werden. Weitere Informationen zur Verwendung von Computer Setup finden Sie im *Computer Setup (F10) Utility Handbuch* auf der CD *Documentation and Diagnostics*.

### Einstellen der Schutzstufe für den Smart Cover Sensor

So stellen Sie die Schutzstufe für den Smart Cover Sensor ein:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie unter **Windows** auf **Start > Beenden > Neu starten**.
2. Drücken Sie sofort nach dem Einschalten des Computers, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10**, um Computer Setup aufzurufen. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten. Halten Sie dann, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10** gedrückt, um das Dienstprogramm aufzurufen.

3. Wählen Sie die Befehlsfolge **Security > Smart Cover > Cover Removal Sensor** (Sicherheit > Smart Cover > Cover Removal Sensor) und dann die gewünschte Sicherheitsstufe.
4. Klicken Sie vor dem 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. Diese Verriegelung verhindert den unbefugten Zugriff auf die inneren Komponenten des Computers. Standardmäßig ist Smart Cover Lock deaktiviert.



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



Das Smart Cover Lock ist als Zusatzoption für einige 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 unter Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie sofort nach dem Einschalten des Computers, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10**, um Computer Setup aufzurufen. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten. Halten Sie dann, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10** gedrückt, um das Dienstprogramm aufzurufen.

3. Wählen Sie die Befehlsfolge **Security > Smart Cover > Cover Lock > Lock** (Sicherheit > Smart Cover > Abdeckungsverriegelung > Aktivieren).
4. Klicken Sie vor dem Beenden auf **File > Save Changes and Exit** (Datei > Änderungen speichern und schließen).

## Deaktivieren von Smart Cover Lock

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie unter Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie sofort nach dem Einschalten des Computers, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10**, um Computer Setup aufzurufen. Drücken Sie die **Eingabetaste**, um ggf. den Titelschirm zu überspringen.



---

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten. Halten Sie dann, wenn die LED-Anzeige des Monitors grün leuchtet, die Taste **F10** gedrückt, um das Dienstprogramm aufzurufen.

---

3. Wählen Sie die Befehlsfolge **Security > Smart Cover > Cover Lock > Unlock** (Sicherheit > Smart Cover > Abdeckungsverriegelung > Deaktivieren).
4. Klicken Sie vor dem 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 das Benutzerkennwort nicht eingeben können, um die Sperre zu deaktivieren, benötigen Sie einen Smart Cover FailSafe-Schlüssel, um die Gehäuseabdeckung öffnen zu können. Sie benötigen den Schlüssel in folgenden Fällen:

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



---

**ACHTUNG:** Der Smart Cover FailSafe-Schlüssel ist ein Spezial-Tool, das von HP angeboten wird. Beugen Sie vor, und bestellen Sie den Schlüssel bei einem Servicepartner, ehe Sie ihn benötigen.

---

So bestellen Sie einen FailSafe-Schlüssel:

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

Weitere Informationen zur Verwendung des Smart Cover FailSafe-Schlüssels finden Sie im *Hardware-Referenzhandbuch* auf der CD *Documentation and Diagnostics*.

## Diebstahlsicherung

Auf der Rückseite des Computers befindet sich ein Kabelschloss zur Diebstahlsicherung, sodass das Gerät an einen festen Gegenstand im Arbeitsbereich angeschlossen werden kann.

Anleitungen mit den entsprechenden Abbildungen finden Sie im *Hardware-Referenzhandbuch* auf der CD *Dokumentation und Diagnose*.

## Fingerabdruckerkennungstechnologie

Die HP Fingerabdruckerkennungstechnologie macht die Eingabe eines Benutzerkennworts überflüssig, erhöht die Netzwerksicherheit, vereinfacht den Anmeldevorgang und reduziert die mit dem Management von Firmennetzwerken verbundenen Kosten. Wegen ihres erschwinglichen Preises ist sie nicht mehr nur High-Tech-Organisationen mit hohen Sicherheitsanforderungen vorbehalten.



Die Unterstützung der Fingerabdruckerkennungstechnologie hängt von dem jeweiligen Modell ab.

---

Weitere Informationen finden Sie unter folgender Adresse:

<http://h18004.www1.hp.com/products/security/>.

## Fehlermeldung und Fehlerbeseitigung

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

Wenn der Computer an ein Netzwerk angeschlossen wird, das mithilfe von HP Client Manager verwaltet wird, gibt er an die Netzwerk-Management-Anwendung eine Fehlermeldung aus. Sie können mithilfe von HP Client Manager Software auch die Remote-Ausführung eines Diagnose-Tools planen, das auf allen verwalteten PCs automatisch ausgeführt wird und einen Übersichtsbericht der fehlgeschlagenen Tests erstellt.

## Drive Protection System

Das Drive Protection System (DPS) ist ein in die Festplatten einiger 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. Diese Informationen können einen Servicepartner bei der Diagnose der Bedingungen unterstützen, die Sie zur Ausführung der DPS-Software veranlasst haben. Anleitungen zur Verwendung von DPS finden Sie im *Fehlerbeseitigungs-Handbuch* auf der CD *Documentation and Diagnostics*.

## **Überspannungsschutz**

Ein integriertes überspannungstolerantes Netzteil erhöht die Zuverlässigkeit in Fällen, in denen der Computer einer unvorhergesehen hohen Spannung ausgesetzt ist. Dieses Netzteil ist so ausgelegt, dass eine Überspannung von bis zu 2000 Volt 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, sodass Sie Maßnahmen ergreifen können, bevor die internen Komponenten beschädigt werden oder Daten verloren gehen.

---

# Index

## A

- Abdeckungsverriegelung, Smart Cover Lock 41
- Abdeckungsverriegelung, Vorsichtsmaßnahme 41
- Aktivieren des Smart Cover Lock 41
- Altiris 7
  - AClient 3
  - Deployment Solution Agent 3
- Ändern des Betriebssystems, Wichtige Informationen 26
- Ändern des Kennworts 35

## B

- Begrenzungszeichen 37
- Benachrichtigung über Produktänderungen 12
- Benutzerdefinierte Software 2
- Bestandsüberwachung 27
- Bestellen eines FailSafe-Schlüssels 43
- Betriebssysteme, Wichtige Informationen 26
- Bootfähiges Gerät
  - DiskOnKey 20 bis 25
  - Erstellen 20 bis 24
  - HP USB Memory Key 20 bis 25
  - USB-Flash-Laufwerk 20 bis 25

## C

- Change Notification 12
- Cloning-Tools, Software 2
- Computer Setup Dienstprogramme 16

## D

- Dantz Retrospect Express 11
- Deaktivieren des Smart Cover Lock 42
- Diagnose-Tool für Festplatten 44
- Disk, Cloning 2
- DiskOnKey
  - siehe auch* HP USB Memory Key
  - Bootfähig 20 bis 25
- Drivelock 38 bis 39
- Dual-State-Netzschalter 25

## E

- Ehemalige Lösungen 13
- Eingeben
  - Kennwort für den Systemstart 33
  - Setup-Kennwort 34
- Erste Konfiguration 2

## F

- FailSafe-Schlüssel
  - Bestellen 43
  - Vorsichtsmaßnahme 42
- Fehlermeldung 44
- Festplatten, Diagnose-Tool 44
- Fingerabdruckererkennungstechnologie 43

## H

- HP Client Management Solutions 7
- HP Client Manager Software 6
- HP Lifecycle-Lösungen 2
- HP Local Recovery 10

HP OpenView Management Suite for  
  Desktops using Radia 8  
HP System Software Manager 5  
HP USB Memory Key  
  *siehe auch* DiskOnKey  
  Bootfähig 20 bis 25

## I

Implementierungs-Tools, Software 2  
Innentemperatur des Computers 45  
Internetadressen *Siehe* Websites

## K

Kabelschloss zur Diebstahlsicherung 43  
Kennwort  
  Ändern 35  
  Löschen 36, 37  
  Setup 32, 34  
  Sicherheit 31  
  Systemstart 33  
Kennwort für den Systemstart  
  Ändern 35  
  Löschen 36  
Konfigurieren des Netzschalters 25

## L

Landesspezifische Unterschiede bei  
  Begrenzungszeichen 37  
Laufwerk, Schutz 44  
Local Recovery 3  
Löschen des Kennworts 36  
Löschen von Kennwörtern 37

## M

MultiBay-Sicherheit 38 bis 39

## N

Netzschalter  
  Dual-State 25  
  Konfigurieren 25  
Netzteil, Überspannungstolerant 45

## P

PC-Implementierung 2  
PCN (Proactive Change Notification) 12  
Preboot Execution Environment (PXE) 4  
Proactive Change Notification (PCN) 12  
PXE (Preboot Execution Environment) 4

## R

Remote System Installation 4  
  Zugriff 4  
Remote-Installation 4  
Remote-ROM-Flash 14  
ROM  
  Flash 14  
  Remote-Flash 14

## S

Schutz der Festplatte 44  
Schutz des ROM-Speichers,  
  Vorsichtsmaßnahme 14  
Setup  
  Erstes 2  
  Replizieren 16  
Setup-Kennwort  
  Ändern 35  
  Eingeben 34  
  Festlegen 32  
  Löschen 36  
Sicherheit  
  DriveLock 38 bis 39  
  Einstellungen, Einrichtung 27  
  Funktionen, Tabelle 28  
  Kennwort 31  
  MultiBay 38 bis 39  
  Smart Cover Lock 41 bis 43  
  Smart Cover Sensor 40  
Smart Cover FailSafe-Schlüssel, Bestellen 43  
Smart Cover Lock 41 bis 43  
  Aktivieren 41

Deaktivieren 42  
Smart Cover Sensor 40  
  Einstellen 40  
  Schutzstufen 40  
Software  
  Aktualisierung und Management 5  
  Altiris AClient 3  
  Altiris Deployment Solution Agent 3  
  Bestandsüberwachung 27  
  Computer Setup Dienstprogramme 16  
  Drive Protection System 44  
  Fehlermeldung und Fehlerbehebung 44  
  HP Local Recovery 3  
  Integration 2  
  Remote System Installation 4  
  Remote-ROM-Flash 14  
  Wiederherstellung 2  
Steuern des Zugriffs auf den Computer 27  
Subscriber's Choice 13  
Systemstart-Kennwort  
  Eingeben 33

**T**

Tabelle 37  
Tastatur-Begrenzungszeichen,  
  Landesspezifische Unterschiede 37  
Temperatur, Im Computer 45  
Thermosensor 45

**U**

Überspannungsschutz 45  
URLs (Websites) *Siehe* Websites  
USB-Flash-Laufwerk, Bootfähig 20 bis 25

**V**

Vorinstalliertes Software-Image 2  
Vorsichtsmaßnahmen  
  Abdeckungsverriegelung 41  
  FailSafe-Schlüssel 42  
  Schutz des ROM-Speichers 14

**W**

Websites  
  Fingerabdruckerkennungstechnologie 43  
  HPQFlash 15  
  PC-Implementierung 2  
  Proactive Change Notification 12  
  Remote ROM Flash 15  
  Replizieren des Setup 19, 20  
  ROM-Flash 14  
  Softwareunterstützung 26  
  Subscriber's Choice 13  
Wiederherstellung, Software 2

**Z**

Zugriff auf Computer, Steuern 27