Desktop Management
Business Desktops

Dokument-Teilenummer: 361202-041

Mai 2004

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

VORSICHT: In dieser Form gekennzeichneter 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 Desktops
Erste Ausgabe (Mai 2004)
Dokument-Teilenummer: 361202-041

Inhalt

Desktop Management

Index

Desktop Management

HP Intelligent Manageability bietet standardbasierte Lösungen zur Verwaltung und Steuerung von Desktops, Workstations und Notebook-PCs in einer Netzwerkumgebung. HP war 1995 mit der Einführung der branchenweit ersten vollständig verwaltbaren Desktop-PCs ein Vorreiter im Bereich Desktop Manageability und ist Inhaber von Patenten für Manageability-Technologie. Seit dieser Zeit ist HP branchenweit bemüht, die Standards und die Infrastruktur zu entwickeln, die für eine effektive Implementierung, Konfiguration und Verwaltung von Desktops, Workstations und Notebook-PCs erforderlich sind. HP arbeitet eng mit branchenführenden Anbietern von Management-Softwarelösungen zusammen, um die Kompatibilität zwischen Intelligent Manageability und diesen Produkten sicherzustellen. Intelligent Manageability ist ein wichtiger Aspekt des umfassenden Engagements von HP, PC Lifecycle-Lösungen für alle vier Phasen des Lebenszyklus eines Desktop-PCs anzubieten – von der Planung, Implementierung und Verwaltung 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.

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 8)
- 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 und Workstations an: HP Client Manager Software, Altiris Client Management Solutions, System Software Manager; Proactive Change Notification und Subscriber’s Choice.

HP Client Manager Software

HP Client Manager Software (HP CMS) unterstützt Kunden von HP beim Management der Hardware ihrer Client-Computer mithilfe folgender Funktionen:

- Ausführliche Anzeigen des Hardwarebestands 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
- Remote-Änderung der Startreihenfolge

Weitere Informationen zu HP Client Manager finden Sie unter http://h18000.www1.hp.com/im/client_mgr.html.

Altiris Client Management Solutions

HP and Altiris bieten gemeinsam umfassende, nahtlos integrierte System-Management-Lösungen an, die die Betriebskosten von HP Client-PCs reduzieren. Die HP Client Manager Software bildet die Grundlage für weitere Altiris Client Management Solutions, mit denen folgende Aufgaben durchgeführt werden können:

- Bestandsverwaltung
  - Einhaltung von Softwarelizenzbestimmungen
  - PC-Tracking und Reporting
  - Pachtvertrags-, Anlagenverfolgung
- Implementierung und Migration
  - Migration von Microsoft Windows XP Professional oder Home Edition
  - Systemimplementierung
  - „Personality“-Migrationen

- Help Desk und Problemlösung
  - Verwalten von Help Desk-Tickets
  - Remote-Fehlersuche
  - Remote-Problemlösung
  - Client-Wiederherstellung
- Software- und Operations-Management
  - Laufendes Desktop Management
  - Implementieren von HP Systemsoftware
  - Self-Healing von Anwendungen

Weitere Informationen sowie Einzelheiten zum Herunterladen einer voll funktionsfähigen 30-Tage-Probeversion der Altiris Lösungen finden Sie unter http://h18000.www1.hp.com/im/prodinfo.html#deploy.

Auf bestimmten Desktop- und Notebook-Modellen ist ein Altiris Management-Agent als Bestandteil des werkseitig installierten Images integriert. Dieser Agent ermöglicht die Kommunikation mit der Altiris Development Solution, die für die Implementierung neuer Hardware oder die „Personality"-Migration auf ein neues Betriebssystem mithilfe einfacher Anleitungen verwendet werden kann. Altiris Lösungen bieten benutzerfreundliche Software-Verteilungsfunktionen. Bei Verwendung zusammen mit dem System Software Manager oder HP Client Manager Software können Administratoren auch die Aktualisierung des ROM-BIOS und der Gerätetreibersoftware von einer zentralen Konsole aus durchführen.

Weitere Informationen finden Sie unter http://h18000.www1.hp.com/im/index.html.

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 dann die betreffende Software 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 besonderes Symbol gekennzeichnet. Rufen Sie zum Herunterladen des Dienstprogramms oder zum Abrufen weiterer Informationen zu SSM die folgende Website auf: http://www.hp.com/go/ssm.

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 Hard- und Software der meisten von Unternehmen genutzten Computer und Server informiert.
- Eine E-Mail mit Informationen, Ratschlägen und Hinweisen für Kunden, Sicherheitsmitteilungen und Treiber-Warnmeldungen für die meisten 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 Technische Kundenunterstützung 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

ROM-Flash

Der Computer verfügt über einen programmierbaren Flash-ROM-Speicher (ROM=Read Only Memory, Nur-Lese-Speicher). Wenn Sie ein Setup-Kennwort in Computer Setup einrichten, können Sie verhindern, dass der ROM-Speicher versehentlich aktualisiert oder überschrieben wird. Dies ist wichtig, um den fehlerfreien Betrieb des Computers sicherzustellen. Zur Aktualisierung des ROM-Speichers können Sie wie folgt vorgehen:

- Bestellen Sie eine aktuelle ROMPaq Diskette von HP.
- Laden Sie die aktuellsten ROMPaq Images auf der HP Treiber- und Support-Website unter der Adresse http://www.hp.com/support/files 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.hp.com/go/ssm.

Remote-ROM-Flash

Remote ROM Flash ermöglicht dem Systemadministrator, den ROM-Speicher von HP Computern direkt von der zentralen Netzwerk-Management-Konsole aus in einem sicheren Rahmen zu aktualisieren. Der Systemadministrator kann diese Aufgabe für mehrere Computer und PCs remote durchführen. Dies bewirkt eine konsistente Implementierung und eine bessere Überwachung der HP PC ROM-Images über das Netzwerk. Darüber hinaus wird eine höherer Produktivität erreicht, und die Total Cost of Ownership werden gesenkt.

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

Das Dienstprogramm HPQFlash wird verwendet, um den ROM-Speicher 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 den Namen des Computers ein, wenn Sie dazu aufgefordert werden.

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.

Einige Modelle unterstützen auch die Wiederherstellung mithilfe einer ROMPaq CD. Bei ausgewählten Modellen sind ISO ROMPaq Images in den ROM Softpaqs zum Herunterladen integriert.

Wenn im Boot-Block ein ungültiger System-ROM-Speicher festgestellt wird, leuchtet die ROTE Betriebs-LED achtmal im Abstand von jeweils einer Sekunde, gefolgt von einer zwei Sekunden langen Pause. Gleichzeitig wird achtmal hintereinander ein akustisches Signal ausgegeben. Eine Meldung wird angezeigt, die angibt, dass das System in den Boot-Block-Wiederherstellungsmodus schaltet (modellabhängig).

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

1. Wenn sich eine Diskette im Diskettenlaufwerk oder eine CD im CD-ROM-Laufwerk befindet, nehmen Sie diese heraus, und schalten Sie den Computer aus.
2. Legen Sie eine ROMPaq Diskette in das Diskettenlaufwerk ein, oder, falls bei diesem Computer möglich, eine ROMPaq CD in das CD-ROM-Laufwerk.
3. Schalten Sie den Computer ein.

   Wenn keine ROMPaq Diskette oder ROMPaq CD gefunden wird, werden Sie aufgefordert, die Diskette bzw. die CD einzulegen und den Computer neu zu starten.

   Wenn ein Setup-Kennwort eingerichtet wurde, leuchtet die LED-Anzeige für die **Feststelltaste**, und Sie werden zur Eingabe des Kennworts aufgefordert.

4. Geben Sie das Setup-Kennwort ein.

   Wenn das System erfolgreich von der Diskette startet und den ROM erfolgreich umprogrammiert hat, schaltet sich die LED-Anzeige der Tastatur ein. Eine lauter werdende Abfolge von akustischen Signalen kennzeichnet zusätzlich den erfolgreichen Abschluss des Vorgangs.

5. Nehmen Sie die Diskette oder CD heraus, und schalten Sie den Computer aus.

6. 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 (falls eine PS/2-Tastatur angeschlossen ist) und ihre Bedeutung sowie die mit jeder Kombination verbundenen Maßnahme.

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

Modus FailSafe Boot Block	LED-Farbe	Tastatur LED-Aktivität	Status/Meldung
Num-Funktion	Grün	Leuchtet	ROMPaq Diskette oder ROMPaq CD nicht vorhanden, defekt, oder Laufwerk nicht bereit.
Feststell-Funktion	Grün	Leuchtet	Kennwort eingeben.
Num-, Feststell- und Roll-Funktion	Grün	Blinkt in Folge, jeweils einmal (Num-, Feststell- oder Roll-Funktion)	Tastatur im Netzwerkmodus gesperrt.
Num-, Feststell- und Roll-Funktion	Grün	Leuchtet	Boot Block ROM-Flash war 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

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 DC7100 Ultra-Slim Desktops auf einen DX6100 Slim Tower.

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 die Taste **F10** und halten Sie sie gedrückt, bis Computer Setup gestartet wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten und die Taste **F10** gedrückt halten, um das Dienstprogramm aufzurufen.

Wenn Sie eine PS/2-Tastatur verwenden, wird möglicherweise eine Tastatur-Fehlermeldung angezeigt, die Sie nicht zu beachten brauchen.

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 die Taste **F10**, und halten Sie sie gedrückt, bis Computer Setup gestartet wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm 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 DC7100 Ultra-Slim Desktops auf einen DX6100 Slim Tower.

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 11).

1. Erstellen Sie eine bootfähige Diskette oder ein bootfähiges USB-Flash-Laufwerk. Siehe „Unterstütztes USB-Flash-Laufwerk“ auf Seite 14, oder „Nicht unterstütztes USB-Flash-Laufwerk“ auf Seite 18.

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 die Taste **F10**, und halten Sie sie gedrückt, bis Computer Setup gestartet wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten und die Taste **F10** gedrückt halten, um das Dienstprogramm aufzurufen.

Wenn Sie eine PS/2-Tastatur verwenden, wird möglicherweise eine Tastatur-Fehlermeldung angezeigt, die Sie nicht zu beachten brauchen.

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 das Dienstprogramm herunterzuladen, rufen Sie die Website http://welcome.hp.com/ support/files 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 Komponenten, wie beispielsweise ein HP USB Memory Key oder DiskOnKey, verfügen über ein vorinstalliertes Image, das ihre Bootfähigkeit erleichtert. 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 18).

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.

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

- Eines der folgenden Systeme:
  - HP Compaq Business Desktop DC7100 Serie
  - HP Compaq Business Desktop DX6100 Serie
  - HP Compaq Business Desktop D530 Serie – Ultra-Slim Desktop, Small Form Factor oder Convertible Minitower
  - Compaq Evo D500 Ultra-Slim Desktop
  - Compaq Evo D510 Convertible Minitower/Small Form Factor

  Je nach BIOS können zukünftige Systeme ebenfalls das Starten von einem USB-Flash-Laufwerk aus unterstützen.

ACHTUNG: Wenn Sie einen Computer verwenden, der oben nicht aufgeführt wurde, müssen Sie sicherstellen, dass in der standardmäßigen Startreihenfolge in Computer Setup das USB-Laufwerk vor dem Festplattenlaufwerk angegeben ist.

- Eines der folgenden Speichermodule:
  - 16 MB HP USB Memory Key
  - 32 MB HP USB Memory Key
  - 32 MB DiskOnKey
  - 64 MB HP USB Memory Key
  - 64 MB DiskOnKey
  - 128 MB HP USB Memory Key
  - 128 MB DiskOnKey
  - 256 MB HP USB Memory Key
  - 256 MB DiskOnKey
- Eine bootfähige DOS-Diskette mit FDISK und SYS. Wenn SYS nicht verfügbar ist, kann FORMAT verwendet werden. Allerdings gehen dann alle auf dem USB-Flash-Laufwerk vorhandenen Dateien verloren.

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 Laufwerkbuchstaben 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 Laufwerkbuchstaben 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 12.

Nicht unterstütztes USB-Flash-Laufwerk

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.

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

- Eines der folgenden Systeme:
  - HP Compaq Business Desktop DC7100 Serie
  - HP Compaq Business Desktop DX6100 Serie
  - HP Compaq Business Desktop D530 Serie – Ultra-Slim Desktop, Small Form Factor oder Convertible Minitower
  - Compaq Evo D500 Ultra-Slim Desktop
  - Compaq Evo D510 Convertible Minitower/Small Form Factor

  Je nach BIOS können zukünftige Systeme ebenfalls das Starten von einem USB-Flash-Laufwerk aus unterstützen.

ACHTUNG: Wenn Sie einen Computer verwenden, der oben nicht aufgeführt wurde, müssen Sie sicherstellen, dass in der standardmäßigen Startreihenfolge in Computer Setup das USB-Laufwerk vor dem Festplattenlaufwerk angegeben ist.

- Eine bootfähige DOS-Diskette mit FDISK und SYS. Wenn SYS nicht verfügbar ist, kann FORMAT verwendet werden. Allerdings gehen dann alle auf dem USB-Flash-Laufwerk vorhandenen Dateien verloren.

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 die Taste **F10**, und halten Sie sie gedrückt, bis Computer Setup gestartet wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

✎ Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten und die Taste **F10** gedrückt halten, um das Dienstprogramm aufzurufen.

Wenn Sie eine PS/2-Tastatur verwenden, wird möglicherweise eine Tastatur-Fehlermeldung angezeigt, die Sie nicht zu beachten brauchen.

---

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 die 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 die Taste **F10**, und halten Sie sie gedrückt, bis Computer Setup gestartet wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm 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 *Documentation* CD.

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 12.

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. ProtectTools Embedded Security verhindert den unbefugten Zugriff auf Daten, überprüft die Systemintegrität und authentifiziert Drittbenutzer, die versuchen, auf das System zuzugreifen. (Weitere Informationen finden Sie im *HP ProtectTools Embedded Security Handbuch* auf der *Documentation* CD.) Sicherheitsfunktionen wie ProtectTools, der Smart Cover Sensor und das Smart Cover Lock, die für bestimmte 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 Systemverwaltungsprogramme weitergeleitet werden, um darüber zu informieren, dass sich jemand unerlaubten Zugang zu den internen Komponenten des Computers verschafft.

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 *Documentation* CD, 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
Setup Password (Setup-Kennwort)	Ermöglicht das Einrichten und Aktivieren des (Administrator)-Setup-Kennworts. ✎ 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. Weitere Informationen finden Sie im *Fehlerbeseitigungs-Handbuch* auf der *Documentation* CD.
Kennwort für den Systemstart	Zum Einrichten und Aktivieren des Kennworts für den Systemstart. Weitere Informationen finden Sie im *Fehlerbeseitigungs-Handbuch* auf der *Documentation* CD.
Password Options (Kennwortoptionen) (Diese Option wird nur angezeigt, wenn ein Kennwort für den Systemstart festgelegt wurde.)	Zur Angabe, ob das Kennwort für den Warmstart **(STRG+ALT+ENTF)** erforderlich sein soll. Weitere Informationen finden Sie im *Handbuch Desktop Management* auf der *Documentation* CD.
Pre-Boot Authorization (PBA)	Zum Aktivieren/Deaktivieren der Smart Card, die anstelle des Kennworts für den Systemstart verwendet wird.

✎ Weitere Informationen zur Verwendung von Computer Setup finden Sie im *Computer Setup (F10) Utility Handbuch* auf der *Documentation* CD.

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

Überblick über die Sicherheitsfunktionen *(Fortsetzung)*

Option	Beschreibung
Smart Cover	Ermöglicht Ihnen folgende Einstellungen: • Aktivieren und Deaktivieren des Smart Cover Sensors. • Aktivieren/Deaktivieren des Cover Removal Sensors. ✎ Mit *Notify User* (Benutzer benachrichtigen) wird der Benutzer benachrichtigt, sobald der Sensor erkannt hat, dass die Abdeckung entfernt wurde. Mit *Setup Password* (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. Diese Funktion wird nur bei bestimmten Modellen unterstützt. Weitere Informationen finden Sie im *Handbuch Desktop Management* auf der *Documentation* CD.
Embedded Security	Ermöglicht Ihnen folgende Einstellungen: • Aktivieren/Deaktivieren der Embedded Security-Funktion. • Zurücksetzen der Funktion auf die voreingestellten Standardeinstellungen. Die Funktion wird nur bei bestimmten Modellen unterstützt. (Weitere Informationen finden Sie im *HP ProtectTools Embedded Security Handbuch* auf der *Documentation* CD.)
Device Security (Gerätesicherheit)	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).
Network Service Boot (Start der Netzwerkdienste)	Aktiviert/deaktiviert die Funktion zum Starten von einem Betriebssystem, das auf einem Netzwerkserver 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.)

✎ Weitere Informationen zur Verwendung von Computer Setup finden Sie im *Computer Setup (F10) Utility Handbuch* auf der *Documentation* CD.

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

Überblick über die Sicherheitsfunktionen *(Fortsetzung)*

Option	Beschreibung
System-IDs	Ermöglicht Ihnen folgende Einstellungen: • Bestandskennung (18-Byte-Kennung) und Eigentümerkennung (80-Byte-Kennung, die während des POST angezeigt werden). Weitere Informationen finden Sie im *Handbuch Desktop Management* auf der *Documentation* CD. • 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.) Landesspezifische Tastatureinstellungen (z. B. Englisch oder Deutsch) für die Eingabe der System-ID.
DriveLock	Ermöglicht die Zuweisung oder Änderung eines Master- oder Benutzerkennworts für MultiBay-Festplatten. (Diese Funktion wird von SCSI-Festplatten nicht unterstützt.) 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. ✎ Diese Option wird nur angezeigt, wenn mindestens ein Laufwerk, das die DriveLock-Funktion unterstützt, mit dem System verbunden ist. Weitere Informationen finden Sie im *Handbuch Desktop Management* auf der *Documentation* CD.

✎ Weitere Informationen zur Verwendung von Computer Setup finden Sie im *Computer Setup (F10) Utility Handbuch* auf der *Documentation* CD.

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

Überblick über die Sicherheitsfunktionen *(Fortsetzung)*

Option	Beschreibung
Master Boot Record Security (MBR-Sicherheit)	Zum Aktivieren oder Deaktivieren der MBR (Master Boot Record) -Sicherheit. Bei Aktivierung dieser Option werden alle Schreibanforderungen an den MBR der aktuellen bootfähigen Festplatte vom BIOS abgelehnt. Bei jedem Einschalten oder Neustart des Computers vergleicht das BIOS den MBR der aktuellen bootfähigen Festplatte mit dem zuvor gespeicherten MBR. Wenn Änderungen erkannt wurden, haben Sie die Möglichkeit, den MBR auf der aktuellen bootfähigen Festplatte zu speichern, den zuvor gespeicherten MBR wiederherzustellen oder die MBR-Sicherheit zu deaktivieren. Sie müssen das Setup-Kennwort kennen, falls ein Kennwort festgelegt wurde. ✎ Deaktivieren Sie die MBR-Sicherheit, bevor Sie die Formatierung oder Partitionierung der aktuellen bootfähigen Festplatte ändern. Bestimmte Festplattendienstprogramme (wie z. B. FDISK und FORMAT) versuchen, den MBR zu aktualisieren. Wenn die MBR-Sicherheit aktiviert ist und der Zugriff auf die Festplatte vom BIOS gesteuert wird, werden Schreibanforderungen an den MBR abgelehnt, und die Dienstprogramme geben Fehlermeldungen aus. Wenn die MBR-Sicherheit aktiviert ist und der Zugriff auf die Festplatte vom Betriebssystem gesteuert wird, werden alle MBR-Änderungen vom BIOS beim nächsten Neustart erkannt, und es wird eine MBR-Warnmeldung angezeigt.

✎ Weitere Informationen zur Verwendung von Computer Setup finden Sie im *Computer Setup (F10) Utility Handbuch* auf der *Documentation* CD.

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

Überblick über die Sicherheitsfunktionen *(Fortsetzung)*

Option	Beschreibung
Save Master Boot Record (MBR speichern)	Speichert eine Sicherungskopie des Master Boot Record der aktuellen bootfähigen Festplatte. Diese Option wird nur angezeigt, wenn die MBR-Sicherheit aktiviert ist.
Restore Master Boot Record (MBR wiederherstellen)	Stellt die aktuelle bootfähige Festplatte anhand der Sicherungskopie des Master Boot Record wieder her. ✎ Diese Option wird nur angezeigt, wenn Folgendes zutrifft: • Die MBR-Sicherheit wurde aktiviert. • Eine Sicherungskopie des MBR ist vorhanden. • Bei der aktuellen bootfähigen Festplatte handelt es sich um die gleiche Festplatte, von der die Sicherungskopie des MBR erstellt wurde. ⚠ **ACHTUNG:** Wenn Sie einen zuvor gespeicherten MBR wiederherstellen, nachdem Änderungen am MBR durch ein Dienstprogramm oder das Betriebssystem vorgenommen wurden, kann auf die Daten der Festplatte unter Umständen nicht mehr zugegriffen werden. Stellen Sie einen zuvor gespeicherten MBR nur dann wieder her, wenn Sie sicher sind, dass der MBR der aktuellen bootfähigen Festplatte beschädigt oder von Viren befallen ist.

✎ Weitere Informationen zur Verwendung von Computer Setup finden Sie im *Computer Setup (F10) Utility Handbuch* auf der *Documentation* CD.

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

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 Embedded Security Handbuch* auf der *Documentation* CD. 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 die Taste **F10**, und halten Sie sie gedrückt, bis Computer Setup gestartet wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten und die Taste **F10** gedrückt halten, um das Dienstprogramm aufzurufen.

Wenn Sie eine PS/2-Tastatur verwenden, wird möglicherweise eine Tastatur-Fehlermeldung angezeigt, die Sie nicht zu beachten brauchen.

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 die Taste **F10**, und halten Sie sie gedrückt, bis Computer Setup gestartet wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten und die Taste **F10** gedrückt halten, um das Dienstprogramm aufzurufen.

Wenn Sie eine PS/2-Tastatur verwenden, wird möglicherweise eine Tastatur-Fehlermeldung angezeigt, die Sie nicht zu beachten brauchen.

---

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 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.

Eingabe eines Setup-Kennworts

Wenn das System mit Embedded Security ausgestattet ist, finden Sie weitere Informationen im *HP ProtectTools Embedded Security Handbuch* auf der *Documentation* CD.

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 die Taste **F10**, und halten Sie sie gedrückt, bis Computer Setup gestartet wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten und die Taste **F10** gedrückt halten, um das Dienstprogramm aufzurufen.

Wenn Sie eine PS/2-Tastatur verwenden, wird möglicherweise eine Tastatur-Fehlermeldung angezeigt, die Sie nicht zu beachten brauchen.

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 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

Wenn das System mit Embedded Security ausgestattet ist, finden Sie weitere Informationen im *HP ProtectTools Embedded Security Handbuch* auf der *Documentation* CD.

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 beim Einschalten des Computers die Taste **F10**, und halten Sie sie gedrückt, bis Computer Setup gestartet wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten und die Taste **F10** gedrückt halten, um das Dienstprogramm aufzurufen.

Wenn Sie eine PS/2-Tastatur verwenden, wird möglicherweise eine Tastatur-Fehlermeldung angezeigt, die Sie nicht zu beachten brauchen.

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 auf dem Bildschirm nicht 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 34. 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* auf der *Documentation* CD.

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 beim Einschalten des Computers die Taste **F10** und halten Sie gedrückt, bis Computer Setup gestartet wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten und die Taste **F10** gedrückt halten, um das Dienstprogramm aufzurufen.

Wenn Sie eine PS/2-Tastatur verwenden, wird möglicherweise eine Tastatur-Fehlermeldung angezeigt, die Sie nicht zu beachten brauchen.

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	-	Koreanisch	/	Taiwanesisch	/
Dänisch	-	Lateinamerikanisch (Spanisch/Portugiesisch)	-	Thailändisch	/
Französisch	!	Norwegisch	-	Türkisch	.
Kan. 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 *Documentation* CD.

Wenn das System mit Embedded Security ausgestattet ist, finden Sie weitere Informationen im *HP ProtectTools Embedded Security Handbuch* auf der *Documentation* CD.

DriveLock

DriveLock ist eine Sicherheitsfunktion, die den unbefugten Zugriff auf Daten von MultiBay-Festplatten verhindert. DriveLock wurde als Erweiterung von Computer Setup implementiert. Die Funktion ist nur verfügbar, wenn DriveLock-fähige Festplattenlaufwerke erkannt werden.

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 für immer gesperrt. Dies stellt für Benutzer, die nicht dem obigen Kundenprofil entsprechen, unter Umständen ein inakzeptables Risiko dar. Für Benutzer, die diesem Profil entsprechen, 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 eine Firmenumgebung geeignet, in der die Computer einiger Benutzer mit MultiBay Festplatten ausgestattet sind. Der Systemadministrator hat die Aufgabe, die MultiBay Festplatte zu konfigurieren, und dazu gehört unter anderem auch das Festlegen des DriveLock-Masterkennworts. 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	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 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 *Documentation* CD.

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 die Taste **F10**, und halten Sie sie gedrückt, bis Computer Setup gestartet wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten und die Taste **F10** gedrückt halten, um das Dienstprogramm aufzurufen.

Wenn Sie eine PS/2-Tastatur verwenden, wird möglicherweise eine Tastatur-Fehlermeldung angezeigt, die Sie nicht zu beachten brauchen.

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 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 unter Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie sofort nach dem Einschalten des Computers die Taste **F10**, und halten Sie sie gedrückt, bis Computer Setup gestartet wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten und die Taste **F10** gedrückt halten, um das Dienstprogramm aufzurufen.

Wenn Sie eine PS/2-Tastatur verwenden, wird möglicherweise eine Tastatur-Fehlermeldung angezeigt, die Sie nicht zu beachten brauchen.

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 die Taste **F10**, und halten Sie sie gedrückt, bis Computer Setup gestartet wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten und die Taste **F10** gedrückt halten, um das Dienstprogramm aufzurufen.

Wenn Sie eine PS/2-Tastatur verwenden, wird möglicherweise eine Tastatur-Fehlermeldung angezeigt, die Sie nicht zu beachten brauchen.

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 *Documentation* CD.

MBR-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. Die MBR (Master Boot Record)-Sicherheitsfunktion erkennt und meldet unbeabsichtigte oder böswillige Änderungen des MBR, die beispielsweise durch Viren oder die unkorrekte Verwendung von bestimmten Festplattendienst-programmen verursacht wurden. Außerdem können Sie den „letzten, als funktionierend bekannten“ 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 unter Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie sofort nach dem Einschalten des Computers die Taste **F10**, und halten Sie sie gedrückt, bis Computer Setup gestartet wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten und die Taste **F10** gedrückt halten, um das Dienstprogramm aufzurufen.

Wenn Sie eine PS/2-Tastatur verwenden, wird möglicherweise eine Tastatur-Fehlermeldung angezeigt, die Sie nicht zu beachten brauchen.

---

3. Wählen Sie **Security > Master Boot Record Security > Enabled (Sicherheit > MBR-Sicherheit > Aktiviert)**.
4. Wählen Sie **Security > Save Master Boot Record (Sicherheit > MBR speichern)**.
5. Klicken Sie vor dem 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 folgende Schritte durchführen:

- Speichern Sie den MBR der aktuellen bootfähigen Festplatte
- Stellen Sie den zuvor gespeicherten MBR wieder her oder
- Deaktivieren Sie die MBR-Sicherheitsfunktion.

Sie benötigen das Setup-Kennwort, falls ein solches Kennwort festgelegt wurde.

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

2000 – Master Boot Record Hard Drive has changed (2000 – Master Boot Record-Festplatte hat sich 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 folgende Schritte durchführen:

- Speichern Sie den MBR der aktuellen bootfähigen Festplatte oder
- Deaktivieren Sie die MBR-Sicherheitsfunktion.

Sie benötigen das Setup-Kennwort, falls ein solches Kennwort festgelegt wurde.

In dem unwahrscheinlichen Fall, dass der zuvor gespeicherte MBR beschädigt wurde, wird 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 folgende Schritte durchführen:

- Speichern Sie den MBR der aktuellen bootfähigen Festplatte oder
- Deaktivieren Sie die MBR-Sicherheitsfunktion.

Sie benötigen das Setup-Kennwort, falls ein solches Kennwort festgelegt 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 der MBR-Sicherheitsfunktion. So deaktivieren Sie die MBR-Sicherheit:

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 die Taste **F10**, und halten Sie sie gedrückt, bis Computer Setup gestartet wird. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer erneut starten und die Taste **F10** gedrückt halten, um das Dienstprogramm aufzurufen.

Wenn Sie eine PS/2-Tastatur verwenden, wird möglicherweise eine Tastatur-Fehlermeldung angezeigt, die Sie nicht zu beachten brauchen.

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

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 *Documentation* CD.

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 bestimmter HP Computer integriertes Diagnose-Tool. Dieses Tool soll die Diagnose 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. Bei jeder Ausführung von DPS werden die Testergebnisse 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 *Documentation* CD.

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

T

U

V

W

Z