Desktop Management
HP zakelijke pc's

Desktop Management

HP zakelijke pc's

Vierde editie, september 2009

Artikelnummer van document: 581009-331

Over deze handleiding

Deze handleiding bevat definities en instructies voor het gebruik van de voorzieningen voor beveiliging en beheer, die op bepaalde modellen vooraf zijn geïnstalleerd.

⚠ **WAARSCHUWING!** Als u de aanwijzingen na dit kopje niet opvolgt, kan dit leiden tot persoonlijk letsel of levensgevaar.

△ **VOORZICHTIG:** Als u de aanwijzingen na dit kopje niet opvolgt, kan dit beschadiging van de apparatuur of verlies van gegevens tot gevolg hebben.

OPMERKING: De tekst na dit kopje biedt belangrijke aanvullende informatie.

Inhoudsopgave

1 Overzicht desktopbeheer

HP Client Management Solutions biedt op standaarden gebaseerde oplossingen voor het beheren en besturen van desktopcomputers, werkstations en notebookcomputers in een netwerkomgeving. HP heeft in 1995 met de introductie van de eerste desktopcomputers die volledig konden worden beheerd, het voortouw genomen op het gebied van desktopbeheer. HP is houder van een patent op technologie voor beheersoftware. Sindsdien heeft de industrie onder leiding van HP gezamenlijke standaarden en infrastructuren ontwikkeld die zijn vereist om desktopcomputers, werkstations en notebookcomputers effectief te kunnen installeren, configureren en beheren. HP ontwikkelt zelf beheersoftware en werkt nauw samen met toonaangevende leveranciers van beheersoftware om de compatibiliteit tussen HP Client Management Solutions en deze beheerapplicaties te waarborgen. HP probeert constant oplossingen te bieden die u kunnen helpen de totale kosten van eigendom en onderhoud van pc's gedurende hun levensduur te beperken. HP Client Management Solutions is hiervan een heel goed voorbeeld.

De belangrijkste functies en voorzieningen van desktopbeheer zijn:

- Eerste configuratie en ingebruikneming
- Systeeminstallatie op afstand
- Updates en beheer van software
- ROM-flash
- Configuratie van de hardwareopties
- Inventarisbeheer en beveiliging
- Foutberichten en foutherstel

OPMERKING: De ondersteuning voor specifieke functies die in deze handleiding worden beschreven, varieert per model of softwareversie.

2 Initiële configuratie en implementatie

De computer wordt geleverd met een vooraf geïnstalleerd image van de systeemsoftware. Na een korte procedure waarin de software wordt "uitgepakt", is de computer gereed voor gebruik.

Desgewenst kunt u het vooraf geïnstalleerde software-image vervangen door een aangepast pakket met systeem- en applicatiesoftware. Aangepaste software kan op verschillende manieren worden geïmplementeerd. Enkele manieren zijn:

- extra softwareapplicaties installeren nadat u het vooraf geïnstalleerde software-image heeft uitgepakt;
- hulpmiddelen voor software-implementatie gebruiken, zoals HP Automation Standard Edition of HP Client Automation Enterprise Edition (op basis van Radia-technologie), waarmee u de vooraf geïnstalleerde software vervangt door een aangepaste software-image;
- de inhoud van een vaste schijf naar een andere vaste schijf kopiëren via een kloonproces.

Wat de beste methode voor implementatie is, hangt af van uw IT-omgeving en IT-processen.

Setup op ROM-basis en ACPI-hardware bieden hulp bij het herstellen van systeemsoftware, configuratiebeheer, het oplossen van problemen en energiebeheer.

HP Client Automation Agent

De beheeragent, die wordt gebruikt door HP Client Automation Standard en Enterprise Editions, is vooraf op de computer geladen. Wanneer deze is geïnstalleerd, wordt communicatie mogelijk met de HP beheerconsole.

Ga als volgt te werk om de HP Client Automation Agent te installeren:

1. Klik op **Start**.
2. Klik op **Alle programma's**.
3. Klik op **HP Manageability**.
4. Klik op het bestand **HP Management Agent Readme** voor de gewenste taal.
5. Volg de instructies in het Readme-bestand om de HP Client Automation Agent te installeren.

De HP Client Automation Agent is een belangrijk infrastructuuronderdeel dat het gebruik van alle HP Client Automation oplossingen mogelijk maakt. Ga voor meer informatie over de andere infrastructuuronderdelen die u nodig heeft voor de implementatie van HP oplossingen voor configuratiebeheer naar http://h20229.www2.hp.com/solutions/ascm/index.html.

HP Client Manager

HP Client Manager (HPCM) is een gratis oplossing ontwikkeld door Symantec voor alle ondersteunde HP zakelijke desktopcomputers, notebookcomputers, werkstationcomputers en HP blade-pc's. HPCM integreert HP hulpmiddelen zoals System Software Manager, HP Instant Support Professional Edition en HP Client Management Interface om een gecentraliseerd model te bieden voor het beheren, volgen en bewaken van alle ondersteunde HP hardware.

HP Client Manager 7.0 is voorzien van een gloednieuwe portalpagina die fungeert als 'one-stop shop', waar de beheerder de volgende beheertaken kan uitvoeren:

- Inventaris
- Waarschuwingen
- BIOS-beheer
- Stuurprogramma-updates
- HP Instant Support Health Scan en Diagnostics uitvoeren
- Geïntegreerde beveiligingstaken uitvoeren
- Algemene HP Health Alert Trend van de afgelopen 3 tot 6 maanden weergeven
- Algemene compatibiliteit van ondersteunde computers met HP Instant Support Health Scan en Diagnostics weergeven
- Samenvatting van HP computers weergeven: een analyse van de ondersteunde desktopcomputers, notebookcomputers, werkstations en HP blade-pc's
- Waarschuwingen weergeven: apparaat, drempel, hardwarestatus
- Rapporten
- Beheertaken voor het bijwerken van HP hulpmiddelen

U kunt HPCM downloaden van http://www.symantec.com/business/theme.jsp door te klikken op **HP Client Manager** onder **Strategic Partner Products** (Strategische partnerproducten). Op de downloadpagina kan tevens een gratis permanente licentie worden verkregen.

HPCM instructievideo's zijn ook beschikbaar op http://www.symantec.com/connect. Zoek naar **HP Client Manager 7.0** voor stapsgewijze video's voor verschillende taken binnen HPCM.

3 Systeeminstallatie op afstand

Met Remote System Installation kunt u het systeem opstarten en instellen met gebruik van software en configuratie-informatie op een netwerkserver, met behulp van PXE (Preboot Execution Environment). De voorziening Remote System Installation wordt meestal gebruikt als hulpmiddel bij het installeren en configureren van systemen, en kan worden gebruikt voor de volgende taken:

- Vaste schijf formatteren
- Software-image installeren op een of meerdere nieuwe pc's
- Het systeem-BIOS in het flash-ROM op afstand bijwerken (ROM-flash op afstand op pagina 14)

  OPMERKING: Er zijn voorzieningen beschikbaar om het systeem-BIOS te flashen vanuit het besturingssysteem Microsoft Windows.

- Instellingen van het systeem-BIOS configureren

U start de systeeminstallatie op afstand door op F12 te drukken zodra de melding **F12 = Network Service Boot** (Opstarten via netwerkservice) tijdens het opstarten rechts onder in het scherm met het HP logo verschijnt. Volg de instructies op het scherm om door te gaan. De standaardopstartvolgorde is een BIOS-configuratie-instelling die u zodanig kunt aanpassen dat het systeem altijd probeert op te starten middels PXE.

4 Software bijwerken en beheren

HP biedt verscheidene hulpmiddelen voor het beheren en bijwerken van software op desktopcomputers, werkstations en notebookcomputers:

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

HP Client Management Interface

Ongeacht de programma's voor systeembeheer die uw IT-afdeling gebruikt, is het belangrijk om zowel de hardware als software goed te beheren om de IT-kosten laag te kunnen houden zodat uw bedrijf flexibel blijft. IT-beheerders kunnen toegang krijgen tot HP Client Management Interface door eenvoudige scripts te schrijven en deze scripts te integreren met een beheeroplossing naar keuze.

Met de HP CMI (HP Client Management Interface) kunnen nieuwe HP zakelijke computers probleemloos in een beheerde IT-omgeving worden geïntegreerd. HP CMI biedt een interface voor eenvoudige integratie van HP zakelijke computers met veelgebruikte hulpmiddelen voor systeembeheer (zoals Microsoft Systems Management Server, IBM Tivoli Software en HP Operations) en eigen beheerapplicaties van bedrijven. Met behulp van HP CMI kunnen hulpmiddelen en applicaties voor systeembeheer een uitgebreide inventaris opvragen van clients, statusinformatie ontvangen en instellingen van het systeem-BIOS beheren, door direct met de clientcomputer te communiceren. Daardoor is er geen agent- of connectorsoftware nodig voor systeemintegratie.

HP Client Management Interface is gebaseerd op industriestandaarden zoals Microsoft Windows Management Interface (MS WMI), Web-Based Enterprise Management (WBEM), System Management BIOS (SMBIOS) en Advanced Configuration and Power Interface (ACPI). HP CMI is een

basistechnologie die gebruikt wordt in HP Client Management Solutions. Met HP CMI geeft HP u de flexibiliteit om zelf te kiezen hoe u uw HP clientcomputers beheert.

Als u HP Client Management Interface gebruikt in combinatie met systeembeheersoftware kunt u het volgende doen:

- Zeer uitgebreide informatie over clients opvragen: gedetailleerde gegevens over processoren, vaste schijven, geheugen, BIOS, stuurprogramma's en sensorgegevens (zoals ventilatorsnelheid, voltage en temperatuur).
- Informatie ontvangen over de gezondheidstoestand van het systeem: u kunt zich aanmelden voor een uitgebreide reeks waarschuwingen met betrekking tot de hardware van clients (bijvoorbeeld overschrijding maximale temperatuur, stilstaande ventilator en wijzigingen in de hardwareconfiguratie), die vervolgens naar de systeembeheerconsole, de applicatie of de lokale clientcomputer worden verzonden. Waarschuwingen worden in real-time verzonden wanneer ze door hardwaregebeurtenissen worden geactiveerd.
- Instellingen van de systeem-BIOS beheren: vanaf uw systeembeheerconsole op afstand F10-functies uitvoeren zoals het instellen en wijzigen van de BIOS-wachtwoorden en de opstartvolgorde op één of alle clientsystemen zonder naar elke computer toe te hoeven gaan.

Voor meer informatie over HP Client Management Interface raadpleegt u http://www.hp.com/go/hpcmi/.

HP SoftPaq Download Manager

HP SoftPaq Download Manager is een gratis, eenvoudig te gebruiken interface voor het zoeken naar en downloaden van software-updates voor de HP clientcomputers in uw computeromgeving. U kunt de softpaqs die u nodig heeft snel vinden, sorteren en selecteren door uw modelnamen, besturingssystemen en taal op te geven. U kunt HP SoftPaq Download Manager downloaden van http://www.hp.com/go/sdm.

HP System Software Manager

HP System Software Manager (SSM) is een gratis hulpprogramma waarmee de installatie op afstand van apparaatstuurprogramma's en BIOS-updates van de HP zakelijke personal computers in uw netwerk geautomatiseerd wordt. SSM bepaalt automatisch (zonder interactie met de gebruiker) het revisieniveau van de op elk clientsysteem geïnstalleerde stuurprogramma's en het BIOS en vergelijkt deze lijst met de systeemsoftware-SoftPaqs die getest en opgeslagen zijn op een centrale bestandenopslaglocatie. SSM werkt vervolgens automatisch down-revision systeemsoftware bij op de netwerk-pc's naar een recenter niveau dat beschikbaar is in de opslaglocatie. Aangezien SSM de distributie van SoftPaq-updates uitsluitend toestaat voor de juiste clientsysteemmodellen, kunnen beheerders erop vertrouwen dat de systeemsoftware met SSM op efficiënte wijze wordt bijgewerkt.

System Software Manager is geschikt voor integratie met diverse hulpmiddelen voor softwaredistributie, zoals HP Client Automation oplossingen, HP Client Manager from Symantec en Microsoft Systems Management Server (SMS). Met SSM kunt u in SSM-indeling verpakte updates distribueren die door uw klanten of door andere fabrikanten zijn gemaakt.

U kunt SSM gratis downloaden van http://www.hp.com/go/ssm.

OPMERKING: SSM biedt momenteel geen ondersteuning voor ROM-flash op afstand op systemen waarop Windows BitLocker Drive Encryption is ingeschakeld en die TPM gebruiken om de BitLocker-sleutels te beschermen, omdat het flashen van het BIOS de handtekening die BitLocker voor het platform heeft gemaakt, ongeldig zou maken. Schakel BitLocker uit via Groepsbeleid om het systeem-BIOS te flashen.

U kunt ondersteuning voor BitLocker inschakelen zonder TPM-maatregelen voor het BIOS, om te voorkomen dat de BitLocker-sleutels ongeldig worden gemaakt. HP raadt u aan een reservekopie van de BitLocker-gegevens veilig te bewaren voor wanneer u het systeem in noodsituaties wilt herstellen.

HP ProtectTools Security Manager

De HP ProtectTools beveiligingssoftware biedt beveiligingsvoorzieningen waarmee u voorkomt dat onbevoegden toegang krijgen tot de computer, netwerken en kritieke gegevens. De volgende softwaremodules bieden verbeterde beveiligingsfuncties, die beschikbaar zijn via HP ProtectTools Security Manager:

HP ProtectTools Security Manager is de console waardoor alle andere modules bereikbaar zijn:

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

HP ProtectTools biedt twee versies die kunnen worden gebruikt: HP ProtectTools Security Manager en HP ProtectTools Administrative Console. In het menu **Start** > **Alle programma's** zijn zowel beheerders- als gebruikersversies beschikbaar.

De softwaremodules die beschikbaar zijn voor uw computer kunnen per model verschillen. Embedded Security for HP ProtectTools is bijvoorbeeld alleen beschikaar voor computers waarop de geïntegreerde beveiligingschip TPM (Trusted Platform Module) is geïnstalleerd.

HP ProtectTools modules kunnen vooraf zijn geïnstalleerd of geladen, of worden gedownload van de HP website. Voor bepaalde HP Pro desktopcomputers is HP ProtectTools verkrijgbaar als after-market optie. Bezoek http://www.hp.com/products/security voor meer informatie.

HP Client Automation Starter en Standard Editions

HP Client Automation is een gebruiksvriendelijke en eenvoudig te implementeren hardware- en softwarebeheeroplossing voor Windows Vista-, Windows XP- en HP Thin Client omgevingen, die een sterke basis biedt voor toekomstige vereisten. De oplossing wordt aangeboden in twee edities:

- De Starter Edition (basiseditie) is een gratis product voor het beheren van HP desktopcomputers, notebookcomputers en werkstations. Het biedt hardware en software, beheer op afstand, HP alert monitoring, HP BIOS- en stuurprogramma-updates, ingratie met HP ProtectTools en toegevoegde ondersteuning voor Intel AMT. De Starter Edition ondersteunt ook de implementatie en het beheer van HP Thin Clients.
- De Standard Edition is beschikbaar tegen betaling en omvat alle functionaliteit van de Starter Edition plus Windows-implementatie en –migratie, patchbeheermogelijkheden, softwaredistributie en gebruiksmeters voor software.

De HP Client Automation Starter en Standard Editions bieden een migratiepad naar de HP Client Automation Enterprise Edition (op basis van Radia-technologie) voor geautomatiseerd beheer van grote, diverse en constant veranderende IT-omgevingen.

Ga voor meer informatie over HP Client Automation oplossingen naar http://www.hp.com/go/client.

HP Client Automation Enterprise Edition

HP Client Automation Enterprise Edition is een oplossing op basis van beleid, waarmee beheerders software en content constant kunnen inventariseren, implementeren, patchen en beheren op diverse clientplatforms. Met HP Client Automation Enterprise Edition kan de IT-professional het volgende doen:

- Het volledige beheerproces voor levensduur automatiseren, van ontdekking, implementatie en voortdurend beheer tot migratie en afdanking.
- Een volledig softwarepakket automatisch implementeren en voortdurend beheren (besturingssystemen, applicaties, patches, instellingen en content).
- Software beheren op bijna ieder willekeurig apparaat, waaronder desktopcomputers, werkstations en notebookcomputers, binnen een heterogene of enkelvoudige infrastructuur.
- Software beheren op de meeste besturingssystemen.

Dankzij voortdurende configuratiebeheer hebben klanten van HP bevestigd dat zij enorme besparingen op hun IT-kosten hebben gedaan, versnelde time-to-market voor software en content hebben gerealiseerd en productievere gebruikers hebben die meer voldoening uit hun werk halen.

Ga voor meer informatie over HP Client Automation oplossingen naar http://www.hp.com/go/client.

HP Client Manager from Symantec

HP Client Manager from Symantec is ontwikkeld met Altiris en gratis verkrijgbaar voor alle ondersteunde HP zakelijke desktopcomputers, notebookcomputers en werkstationmodellen. SSM is geïntegreerd in HP Client Manager en maakt het volgen, bewaken en beheren van de hardwareonderdelen van HP clientsystemen mogelijk.

U kunt HP Client Manager from Symantec gebruiken om het volgende te doen:

- Waardevolle hardware-informatie opvragen over bijvoorbeeld processor-, geheugen-, video- en beveiligingsinstellingen.
- Systeemstatus bewaken om problemen preventief op te lossen.
- Automatisch stuurprogramma's en BIOS-updates ontvangen en installeren zonder elke pc te hoeven bezoeken.
- BIOS- en beveiligingsinstellingen op afstand configureren.
- Hardwareproblemen snel oplossen met behulp van geautomatiseerde processen.

Door strakke integratie met HP Instant Support is minder tijd nodig voor het oplossen van hardwareproblemen.

- Diagnostische middelen: hiermee kunt u op afstand rapportages uitvoeren en weergeven op HP desktopcomputers, notebookcomputers en werkstations.
- Systeemgezondheid scannen: hiermee controleert u bekende hardwareproblemen in de geïnstalleerde HP clientsystemen.
- Active Chat: hiermee brengt u een verbinding tot stand met een HP Business Partner.
- HP Knowledgebase: hiermee kunt u informatie van deskundigen raadplegen.
- Geautomatiseerd verzamel- en afleverproces voor SoftPaq's voor het snel oplossen van hardwareproblemen.
- Systemen voor identificatie, inventarisatie en initialisatie met ingebouwde HP ProtectTools beveiligings-chip.
- Mogelijkheid voor het lokaal weergeven van gezondheidswaarschuwingen op het clientsysteem.
- Rapporteren van basis-inventarisgegevens over niet-HP clients.
- TPM-beveiligingschip instellen en configureren.
- Back-up en herstel voor clients centraal plannen.
- Toegevoegde ondersteuning voor Intel AMT-beheer.

Ga voor meer informatie over HP Client Manager from Symantec naar http://www.hp.com/go/clientmanager.

Altiris Client Management Suite

Altiris Client Management Suite is een gebruiksvriendelijke oplossing voor het beheer van de volledige levenscyclus van software op desktopcomputers, notebookcomputers en werkstations. Client Management Suite bevat de volgende Altiris-producten:

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

- Application Metering Solution
- Application Management Solution
- Carbon Copy Solution

Ga voor meer informatie over Altiris Client Management Suite naar http://www.symantec.com/business/client-management-suite.

HP Client Catalog for Microsoft System Center & SMS Products

Met de HP Client Catalog kunnen IT-professionals die met Microsoft-producten werken de implementatie van HP software-updates (Softpaqs) op HP zakelijke personal computers volledig automatiseren. Het catalogusbestand bevat gedetailleerde platforminformatie over HP zakelijke desktopcomputers, notebookcomputers en werkstations. Het programma kan worden gebruikt in combinatie met de inventaris- en updatevoorzieningen van Microsoft-producten om automatisch driver-updates en patches te bieden voor beheerde HP clientcomputers.

HP Client Catalog ondersteunt onder andere de volgende Microsoft-producten:

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

Kijk voor meer informatie over HP Client Catalog for SMS op http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html.

Technologie voor beheer op afstand

Computermodellen kunnen zijn voorzien van vPro-technologie of een standaardtechnologie. Beide zorgen voor betere ontdekking, reparatie en bescherming van computermiddelen in een netwerk. Beide technologieën zorgen er bovendien voor dat computers kunnen worden beheerd wanneer ze zijn in- of uitgeschakeld en wanneer het besturingssysteem is vastgelopen.

De drie vormen van beheer op afstand die beschikbaar zijn op zakelijke desktopcomputers, zijn Alert Standard Format (ASF), Intel Active Management Technology (AMT) en Desktop and mobile Architecture for Systems Hardware (DASH).

De voorzieningen van de technologie voor beheer op afstand omvatten:

- Netwerk ontdekken
- Hardware-inventarisatiegegevens
- Platformstatus bewaken
- Energiebeheer: hiermee schakelt u de stroom in of uit of kunt u computers uitschakelen en direct weer inschakelen als het systeem hangt.

- Diagnose en reparatie op afstand
  - Omleiding van tekstconsole: hiermee kunt u de console bedienen vanaf een pc op afstand tijdens de opstartfase.
  - Omleiding van media: hiermee kunt u het systeem opstarten vanaf een opstartdrive, -schijf of –ISO-image op afstand (de twee varianten hiervan zijn IDE-Redirect (IDE-R) op AMT-platforms en USB Media Redirection).
- Isoleren en herstellen van de hardware: hiermee beperkt of beëindigt u bij virusactiviteit de toegang van de pc tot het netwerk.
- Volgen en controleren van platformgebeurtenissen
- Beheerportal via geïntegreerde webserver voor toegang en configuratie op afstand
- Technologieën voor beheer op afstand zijn geïntegreerd in de beheerconsolepartners van HP

OPMERKING: Niet alle hierboven vermelde voorzieningen zijn beschikbaar op alle platforms.

Intel Management Engine configureren

OPMERKING: Voor een overzicht van Intel vPro-technologie bezoekt u http://www.intel.com/vpro.

Raadpleeg voor specifieke informatie van HP over Intel vPro-technologie de whitepapers op http://www.hp.com/support. Selecteer uw land/regio en taal, selecteer **Bekijk supportinformatie of los een probleem op**, typ het modelnummer van de computer en druk op Enter. Klik in de categorie **Resources** (Bronnen) op **Manuals (guides, supplements, addendums, etc)** (Handleidingen (gidsen, supplementen, enzovoort)). Klik bij **Quick jump to manuals by category** (Snel naar handleidingen per categorie) op **White papers** (Whitepapers).

De beschikbare beheertechnologieën zijn onder andere:

- AMT (inclusief DASH 1.0)
- ASF
- DASH 1.1 (met gebruik van Broadcom NIC)

ASF en AMT mogen niet tegelijkertijd worden geconfigureerd, maar worden wel allebei ondersteund.

Ga als volgt te werk om Intel vPro-systemen voor AMT of ASF te configureren:

1. Zet de computer aan of start de computer opnieuw op. Selecteer hiervoor in Microsoft Windows **Start** > **Uitschakelen** > **Opnieuw opstarten**.
2. Druk zodra de computer is ingeschakeld op de sneltoets Ctrl+P, voordat het besturingssysteem wordt geladen.

   OPMERKING: Als u niet op het juiste moment op Ctrl+P drukt, start u de computer opnieuw op en drukt u op Ctrl+P voordat het besturingssysteem wordt geladen, om het hulpprogramma te openen.

Met deze sneltoets opent u het hulpprogramma Intel Management Engine BIOS Execution (MEBx). Met dit hulpprogramma kan de gebruiker diverse aspecten van de beheertechnologie configureren. Hieronder wordt een aantal configuratieopties weergegeven:

- Main Menu (Hoofdmenu)
  - Intel ® ME Configuration (Intel ® ME-configuratie)
  - Intel ® AMT Configuration (Intel ® AMT-configuratie)
  - Change Intel ® ME Password (Intel ® ME-wachtwoord wijzigen)
  - Exit (Afsluiten)
- Intel ® ME Platform Configuration (Intel ® ME-platformconfiguratie)
  - Intel ® ME State Control (enable/disable) (Intel ® ME-statuscontrole (inschakelen/uitschakelen))
  - Intel ® ME Firmware Local Update (enable/disable) (Lokale Intel ® ME-firmware-update (inschakelen/uitschakelen))
  - Intel ® ME Features Control (Intel ® ME-voorzieningenbeheer)
  - Intel ® ME Power Control (Intel ® ME-energiebeheer)
- Intel ® AMT Configuration (Intel ® AMT-configuratie)
  - Host Name (Hostnaam)
  - TCP/IP
  - Provision Model (Enterprise, SMB) (Instellingenmodus (Enterprise, SMB))
  - Setup and Configuration (Instellingen en configuratie)
  - Un-Provision (Standaardinstellingen herstellen)
  - SOL/IDE-R (enable/disable) (SOL/IDE-R (inschakelen/uitschakelen))
  - Password Policy (Wachtwoordbeleid)
  - Secure Firmware Update (enable/disable) (Veilige firmware-update (inschakelen/uitschakelen))
  - Set PRTC (PRTC instellen)
  - Idle Timeout (Time-out voor inactiviteit)
- Change Intel ® ME Password (Intel ® ME-wachtwoord wijzigen). HP adviseert om dit wachtwoord te wijzigen. Het standaardwachtwoord is **admin**.

De beheerder moet gebruikmaken van een console op afstand die ondersteuning biedt voor AMT, om AMT-systemen op afstand te beheren. Beheerconsoles voor bedrijven zijn verkrijgbaar bij leveranciers als HP, Altiris en Microsoft SMS. In de SMB-modus biedt de client een internetbrowser-interface. Als u deze functie wilt gebruiken, opent u een browser van een ander systeem op het netwerk en typt u `http://host_name:16992` waarbij `host_name` de aan het systeem toegewezen naam is. In plaats van de hostnaam kan ook het IP-adres worden gebruikt.

Ga als volgt te werk om systemen met een NIC met Broadcom DASH-mogelijkheden te configureren:

Zoek naar actuele documentatie op de website http://www.hp.com. Selecteer onder **Productondersteuning** uw specifieke model en selecteer **Manuals** (Handleidingen) en vervolgens **White papers** die betrekking hebben op DASH of de Broadcom NIC.

Verdiem Surveyor

Verdiem Surveyor is een oplossing waarmee u de energiekosten van pc's kunt beheren. Surveyor meet en meldt hoeveel energie elke pc verbruikt. Daarnaast kunnen de voedingsinstellingen van de pc's worden geregeld, zodat beheerders eenvoudig energiebesparende strategieën in het gehele netwerk kunnen implementeren. U kunt een HP SoftPaq met de Surveyor-agent downloaden van de ondersteuningswebsite van HP en installeren op ondersteunde commerciële desktopmodellen. Surveyor-licenties voor pc-beheer zijn verkrijgbaar via uw HP vertegenwoordiger.

HP Proactive Change Notification

Het programma Proactive Notification maakt gebruik van de website Subscriber's Choice om proactief en automatisch het volgende te doen:

- U ontvangt per e-mail PCN-berichten (Proactive Change Notification) waarmee u tot 60 dagen van tevoren wordt ingelicht over hardware- en softwarewijzigingen met betrekking tot de meeste commercieel verkrijgbare computers en servers.
- U ontvangt e-mailberichten met Customer Bulletins, Customer Advisories, Customer Notes, Security Bulletins en Driver Alerts voor de meeste commercieel verkrijgbare computers en servers.

U definieert uw eigen profiel, zodat u alleen informatie ontvangt die betrekking heeft op uw specifieke IT-omgeving. Voor meer informatie over Proactive Change Notification en om uw eigen profiel te maken, bezoekt u http://h30046.www3.hp.com/subhub.php.

Subscriber's Choice

Subscriber's Choice is een speciale service van HP.

Op basis van uw profiel ontvangt u van HP op maat gemaakte producttips, informatieve artikelen, kennisgevingen van nieuwe stuurprogramma's en/of informatie over productondersteuning.

Via de Driver and Support Alerts/Notifications van Subscriber’s Choice ontvangt u e-mailberichten die u erop wijzen dat de informatie waarop u via uw profiel bent geabonneerd, gereed is om online te worden bekeken of gedownload. Voor meer informatie over Subscriber’s Choice en voor het maken van een persoonlijk profiel, bezoekt u http://h30046.www3.hp.com/subhub.php.

Verouderde oplossingen

Twee softwarepakketten, Altiris Local Recovery en Dantz Retrospect, worden niet meer geleverd bij HP zakelijke desktopcomputers, notebookcomputers of werkstations.

5 ROM-flash

Het BIOS van de computer bevindt zich in een programmeerbaar flash-ROM (alleen-lezen geheugen). U kunt voorkomen dat het ROM per ongeluk wordt bijgewerkt of overschreven door een instelwachtwoord in te stellen in Computer Setup (Computerinstellingen). Dit is van belang om de bedrijfsintegriteit van de computer te waarborgen. Als u het BIOS wilt upgraden, kunt u de recentste BIOS-images downloaden van de pagina Ondersteuning en drivers op http://www.hp.com/support/files.

△ **VOORZICHTIG:** Definieer een instelwachtwoord om het ROM optimaal te beveiligen. Met het instelwachtwoord worden ongeautoriseerde upgrades van het ROM voorkomen. Met System Software Manager kan de beheerder het instelwachtwoord gelijktijdig instellen op een of meerdere pc's. Ga voor meer informatie naar http://www.hp.com/go/ssm.

ROM-flash op afstand

Met een ROM-flash op afstand kan de systeembeheerder het BIOS van HP computers op afstand veilig bijwerken vanaf de centrale beheerdersconsole. Doordat de systeembeheerder deze taak op afstand kan uitvoeren voor meer pc's tegelijk, is een consistent gebruik van en betere controle op HP PC BIOS-versies in het gehele netwerk mogelijk. Bovendien leidt dit tot een hogere productiviteit en lagere onderhoudskosten.

OPMERKING: SSM biedt momenteel geen ondersteuning voor ROM-flash op afstand op systemen waarop Windows BitLocker Drive Encryption is ingeschakeld en die TPM gebruiken om de BitLocker-sleutels te beschermen, omdat het flashen van het BIOS de handtekening die BitLocker voor het platform heeft gemaakt, ongeldig zou maken. Schakel BitLocker uit via Groepsbeleid om het systeem-BIOS te flashen.

De computer moet zijn ingeschakeld of op afstand worden geactiveerd om van de flash-ROM-upgrade te kunnen profiteren.

Raadpleeg voor meer informatie over ROM-flash op afstand de HP Client Manager software of System Software Manager op http://www.hp.com/go/ssm/.

HPQFlash

Met het hulpprogramma HPQFlash wordt het systeem-BIOS van afzonderlijke pc's vanuit een Windows-besturingssysteem lokaal bijgewerkt of hersteld.

Ga voor meer informatie over HPQFlash naar http://www.hp.com/support/files en voer het modelnummer van de computer in wanneer daarom wordt gevraagd.

6 Boot Block Emergency Recovery Mode

De Boot Block Emergency Recovery Mode (Herstelmodus voor noodsituaties met opstartblok) zorgt ervoor dat het systeem zich kan herstellen in het onwaarschijnlijke geval dat zich een storing voordoet bij de ROM-flash. Als zich tijdens een BIOS-upgrade bijvoorbeeld een stroomstoring voordoet, zou de ROM-flash niet volledig zijn. Hierdoor zou het systeem-BIOS onbruikbaar worden. Het opstartblok is een tegen flashen beveiligd gedeelte van het ROM dat code bevat die bij het inschakelen van het systeem controleert of de systeem-BIOS-versie geldig is.

- Als de versie van het systeem-BIOS geldig is, wordt het systeem normaal gestart.
- Als de versie van het systeem-BIOS niet geldig is, biedt een failsafe Boot Block BIOS voldoende ondersteuning om te zoeken naar verwijderbare media voor BIOS-imagebestanden. Als een geschikt BIOS-imagebestand wordt aangetroffen, wordt het automatisch in het ROM geflasht.

Als een ongeldige BIOS-versie wordt gedetecteerd, knippert het aan/uit-lampje 8 maal in de kleur rood met tussenpozen van 1 seconde. Tegelijkerheid laat het systeem 8 keer een pieptoon horen. Als het gedeelte van het systeem-ROM dat de ROM-versie van de video-optie bevat niet beschadigd is, wordt **Boot Block Emergency Recovery Mode** op het scherm weergegeven.

In de herstelstand voor noodsituaties kunt u het systeem als volgt herstellen:

1. Schakel de stroom uit.
2. Plaats een cd of USB-flashapparaat met in de hoofddirectory het gewenste BIOS-imagebestand.

   OPMERKING: Het medium moet zijn geformatteerd met het FAT12-, FAT16- of FAT32-bestandssysteem.

3. Zet de computer aan.

   Als geen geschikt BIOS-image wordt aangetroffen, wordt u gevraagd om een medium met een BIOS-imagebestand te plaatsen.

   Als het gelukt is om het ROM te herprogrammeren, wordt het systeem automatisch uitgeschakeld.

4. Verwijder de media waarmee u het BIOS heeft bijgewerkt.
5. Schakel de computer in om deze opnieuw op te starten.

OPMERKING: BitLocker voorkomt dat Windows Vista opstart wanneer er zich in de optischeschijfeenheid een cd bevindt met het BIOS-imagebestand. Als BitLocker is ingeschakeld, verwijdert u deze cd voordat u Windows Vista probeert te starten.

7 Setup kopiëren

De volgende procedures bieden een beheerder de mogelijkheid om op eenvoudige wijze een computerconfiguratie te kopiëren naar andere computers van hetzelfde type. Hierdoor kunnen meerdere computers sneller en consistenter worden geconfigureerd.

OPMERKING: Voor beide procedures is een diskettedrive of een ondersteunde USB-flashdrive benodigd.

OPMERKING: System Software Manager (SSM) kan worden gebruikt om computerinstellingen te kopiëren vanuit het besturingssysteem Windows. Raadpleeg voor meer informatie de gebruikershandleiding van SSM op http://www.hp.com/go/ssm.

Kopiëren naar één computer

VOORZICHTIG: Configuraties verschillen per computermodel. Als het model van de broncomputer niet overeenkomt met dat van de doelcomputer, kan het bestandssysteem beschadigd raken. Kopieer bijvoorbeeld nooit de configuratie van een dc7xxx pc naar een dx7xxx pc.

1. Selecteer de installatieconfiguratie die u wilt kopiëren. Zet de computer uit. Selecteer hiervoor in Windows **Start** > **Uitschakelen** > **Uitschakelen**.
2. Plaats nu het USB-flashapparaat, als u dit gebruikt.
3. Zet de computer aan.
4. Druk zodra de computer is ingeschakeld op de sneltoets F10, voordat het besturingssysteem wordt geladen, om Computer Setup (Computerinstellingen) te openen. Druk op Enter om een eventueel beginscherm over te slaan.

   OPMERKING: Als u niet op het juiste moment op F10 drukt, start u de computer opnieuw op en drukt u op F10 voordat het besturingssysteem wordt geladen, om het hulpprogramma te openen.
5. Als u een diskette gebruikt, plaatst u deze nu.
6. Klik op **File** (Bestand) > **Replicated Setup** (Gekopieerde configuratie) > **Save to Removable Media** (Opslaan naar verwijderbare media). Volg de instructies op het scherm om de configuratiediskette of het USB-flashapparaat te maken.
7. Zet de computer die u wilt configureren uit en plaats de configuratiediskette of het USB-flashapparaat.
8. Zet de computer weer aan.
9. Druk zodra de computer is ingeschakeld op de sneltoets F10, voordat het besturingssysteem wordt geladen, om Computer Setup (Computerinstellingen) te openen. Druk op Enter om een eventueel beginscherm over te slaan.

10. Klik op **File** (Bestand) > **Replicated Setup** (Gekopieerde configuratie) > **Restore from Removable Media** (Herstellen vanaf verwijderbaar medium) en volg de instructies op het scherm.

11. Start de computer opnieuw wanneer de configuratie voltooid is.

Kopiëren naar meerdere computers

△ **VOORZICHTIG:** Configuraties verschillen per computermodel. Als het model van de broncomputer niet overeenkomt met dat van de doelcomputer, kan het bestandssysteem beschadigd raken. Kopieer bijvoorbeeld nooit de configuratie van een dc7xxx PC naar een dx7xxx PC.

Bij deze methode duurt de voorbereiding van de configuratiediskette of het USB-flashapparaat wat langer, maar daar staat tegenover dat het kopiëren van de configuratie naar de doelcomputers aanzienlijk sneller verloopt.

OPMERKING: Voor deze procedure of wanneer u een opstartbaar USB-flashapparaat wilt maken, is een opstartdiskette vereist. Als Windows XP niet beschikbaar is voor het maken van een opstartdiskette, kunt u de methode gebruiken voor het kopiëren naar één computer (zie Kopiëren naar één computer op pagina 16).

1. Maak een opstartdiskette of USB-flashapparaat. Zie Ondersteunde USB-flashmedia op pagina 18 of Niet-ondersteunde USB-flashmedia op pagina 19.

   △ **VOORZICHTIG:** Niet alle computers kunnen vanaf een USB-flashapparaat worden opgestart. Als het USB-apparaat in de opstartvolgorde van Computer Setup (Computerinstellingen) eerder wordt vermeld dan de vaste schijf, kan de computer vanaf een USB-flashapparaat worden opgestart. Gebruik in alle andere gevallen een opstartdiskette.

2. Selecteer de installatieconfiguratie die u wilt kopiëren. Zet de computer uit. Selecteer hiervoor in Windows **Start** > **Uitschakelen** > **Uitschakelen**.

3. Plaats nu het USB-flashapparaat, als u dit gebruikt.

4. Zet de computer aan.

5. Druk zodra de computer is ingeschakeld op de sneltoets F10, voordat het besturingssysteem wordt geladen, om Computer Setup (Computerinstellingen) te openen. Druk op Enter om een eventueel beginscherm over te slaan.

   OPMERKING: Als u niet op het juiste moment op F10 drukt, start u de computer opnieuw op en drukt u op F10 voordat het besturingssysteem wordt geladen, om het hulpprogramma te openen.

6. Als u een diskette gebruikt, plaatst u deze nu.

7. Klik op **File** (Bestand) > **Replicated Setup** (Gekopieerde configuratie) > **Save to Removable Media** (Opslaan naar verwijderbare media). Volg de instructies op het scherm om de configuratiediskette of het USB-flashapparaat te maken.

8. Download een BIOS-hulpprogramma voor het kopiëren van de configuratie (repset.exe) en kopieer dit naar de configuratiediskette of naar het USB-flashapparaat. Ga naar http://welcome.hp.com/country/us/en/support.html en typ het modelnummer van de computer om dit hulpprogramma te downloaden.

9. Maak op de configuratiediskette of op het USB-flashapparaat een autoexec.bat-bestand met de volgende opdracht:

   ```
   repset.exe
   ```

10. Zet de computer die u wilt configureren uit. Plaats de configuratiediskette of het USB-flashapparaat en zet de computer weer aan. Het configuratiehulpprogramma wordt automatisch uitgevoerd.

11. Start de computer opnieuw wanneer de configuratie voltooid is.

Opstartapparaat maken

Ondersteunde USB-flashmedia

Ondersteunde apparaten bevatten een vooraf geïnstalleerd image waarmee ze gemakkelijk opstartbaar kunnen worden gemaakt. Alle USB-flashmedia van HP en Compaq en van de meeste andere fabrikanten beschikken over dit vooraf geïnstalleerde image. Als het USB-flashapparaat dat u gebruikt niet van een dergelijk image is voorzien, gebruikt u de procedure die later in dit gedeelte wordt beschreven (zie Niet-ondersteunde USB-flashmedia op pagina 19).

Als u een opstartbaar USB-flashapparaat wilt maken, heeft u het volgende nodig:

- Een ondersteund USB-flashapparaat.
- Een DOS-opstartdiskette met de programma's FDISK en SYS. (Als SYS niet beschikbaar is, kan FORMAT worden gebruikt. Dit betekent echter dat alle bestaande bestanden op het USB-flashapparaat verloren gaan.)
- Een pc die vanaf een USB-flashapparaat kan worden opgestart.

△ **VOORZICHTIG:** Enkele oudere pc-modellen kunnen mogelijk niet vanaf een USB-flashapparaat worden opgestart. Als het USB-apparaat in de opstartvolgorde van Computer Setup (Computerinstellingen) eerder wordt vermeld dan de vaste schijf, kan de computer vanaf een USB-flashapparaat worden opgestart. Gebruik in alle andere gevallen een opstartdiskette.

1. Zet de computer uit.
2. Plaats het USB-flashapparaat in een van de USB-poorten van de computer en verwijder alle andere USB-opslagapparaten met uitzondering van de USB-diskettedrives.
3. Plaats een DOS-opstartdiskette met FDISK.COM en SYS.COM of FORMAT.COM in een diskettedrive en zet de computer aan om de DOS-diskette op te starten.
4. Voer FDISK uit vanaf de **A:**-prompt door `FDISK` te typen en op Enter te drukken. Wanneer u daarom wordt gevraagd, klikt u op **Yes** (Ja, **Y**) om ondersteuning voor grote schijven in te schakelen.
5. Typ keuze [`5`] om de stations in het systeem weer te geven. Het USB-flashapparaat is het station met een formaat dat het meest overeenkomt met een van de vermelde stations. Meestal is dit het laatste station van de lijst. Let op de letter van het station.

   Station voor USB-flashapparaat: _____

   △ **VOORZICHTIG:** Als een station niet overeenkomt met het USB-flashapparaat, mag u niet doorgaan. Het is mogelijk dat gegevens verloren gaan. Controleer of zich in de USB-poorten geen opslagapparaten bevinden. Als dat wel het geval is, verwijdert u ze, start u de computer opnieuw op en gaat u verder vanaf stap 4. Als u geen opslagapparatuur vindt, betekent dit dat het USB-flashapparaat niet ondersteund wordt of dat het defect is. Probeer NIET het USB-flashapparaat toch opstartbaar te maken.

6. Sluit FDISK af door te drukken op de Esc-toets om naar de prompt **A:** terug te keren.

7. Als uw DOS-opstartdiskette SYS.COM bevat, gaat u naar stap 8. Ga anders naar stap 9.

8. Typ achter de prompt **A:** `SYS x:` waarbij x staat voor de eerder genoemde stationsletter.

   △ **VOORZICHTIG:** Zorg ervoor dat u de juiste stationsletter heeft ingevoerd voor het USB-flashapparaat.

   Nadat de systeembestanden zijn overgebracht, keert SYS terug naar prompt **A:**. Ga verder met stap 13.

9. Kopieer de bestanden die u wilt houden van uw USB-flashapparaat naar een tijdelijke directory op een ander station (bijvoorbeeld de interne vaste schijf van het systeem).

10. Typ achter de prompt **A:** `FORMAT /S X:` waarbij `X` staat voor de eerder vermelde stationsletter.

    △ **VOORZICHTIG:** Zorg ervoor dat u de juiste stationsletter heeft ingevoerd voor het USB-flashapparaat.

    FORMAT geeft een aantal berichten weer en vraagt elke keer of u verder wilt gaan. Druk elke keer op `Y`. FORMAT formatteert de USB-flashmedia, voegt de systeembestanden toe en vraagt om een naam voor het volume.

11. Druk op Enter als u geen label wilt invoeren of voer een label in.

12. Kopieer de bestanden die u in stap 9 heeft opgeslagen terug naar het USB-flashapparaat.

13. Verwijder de diskette en start de computer opnieuw op. De computer wordt opgestart vanaf het USB-flashapparaat dat C als stationsletter krijgt.

   OPMERKING: De standaardopstartvolgorde varieert per computer en kan in het hulpprogramma Computer Setup (Computerinstellingen) worden gewijzigd.

   Als u een DOS-versie van Windows 9x heeft gebruikt, krijgt u waarschijnlijk even een scherm met Windows-logo te zien. Als u dit scherm niet wilt, voegt u een leeg bestand, LOGO.SYS, toe aan de hoofddirectory van het USB-flashapparaat.

Ga terug naar Kopiëren naar meerdere computers op pagina 17.

Niet-ondersteunde USB-flashmedia

Als u een opstartbaar USB-flashapparaat wilt maken, heeft u het volgende nodig:

- Een USB-flashapparaat.
- Een DOS-opstartdiskette met de programma's FDISK en SYS. (Als SYS niet beschikbaar is, kan FORMAT worden gebruikt. Dit betekent echter dat alle bestaande bestanden op het USB-flashapparaat verloren gaan.)
- Een pc die vanaf een USB-flashapparaat kan worden opgestart.

△ **VOORZICHTIG:** Enkele oudere pc-modellen kunnen mogelijk niet vanaf een USB-flashapparaat worden opgestart. Als het USB-apparaat in de opstartvolgorde van Computer Setup (Computerinstellingen) eerder wordt vermeld dan de vaste schijf, kan de computer vanaf een USB-flashapparaat worden opgestart. Gebruik in alle andere gevallen een opstartdiskette.

1. Als zich PCI-kaarten in het systeem bevinden met daaraan gekoppelde SCSI-, ATA RAID- of SATA-eenheden, schakelt u de computer uit en haalt u de stekker uit het stopcontact.

   △ **VOORZICHTIG:** De stekker MOET uit het stopcontact worden gehaald.

2. Open vervolgens de computer en verwijder de PCI-kaarten.
3. Plaats het USB-flashapparaat in een van de USB-poorten van de computer en verwijder alle andere USB-opslagapparaten met uitzondering van de USB-diskettedrives. Sluit de behuizing van de computer.
4. Sluit het netsnoer weer aan en zet de computer aan.
5. Druk zodra de computer is ingeschakeld op de sneltoets F10, voordat het besturingssysteem wordt geladen, om Computer Setup (Computerinstellingen) te openen. Druk op Enter om een eventueel beginscherm over te slaan.

   OPMERKING: Als u niet op het juiste moment op F10 drukt, start u de computer opnieuw op en drukt u op F10 voordat het besturingssysteem wordt geladen, om het hulpprogramma te openen.

6. Ga naar **Advanced** (Geavanceerd) > **PCI Devices** (PCI-apparaten) om de PATA- en SATA-controllers uit te schakelen. Onthoud bij het uitschakelen van de SATA-controller aan welke IRQ de controller is toegewezen. In een latere stap moet de IRQ namelijk opnieuw worden toegewezen. Sluit Computer Setup (Computerinstellingen) af en bevestig de wijzigingen.

   SATA IRQ: _____

7. Plaats een DOS-opstartdiskette met FDISK.COM en SYS.COM of FORMAT.COM in een diskettedrive en zet de computer aan om de DOS-diskette op te starten.
8. Start FDISK en verwijder eventuele partities op het USB-flashapparaat. Maak een nieuwe partitie en markeer deze als actief. Druk op de toets Esc om FDISK af te sluiten.
9. Als het systeem na het afsluiten van FDISK niet opnieuw werd opgestart, drukt u op Ctrl+Alt+Del om opnieuw op te starten vanaf de DOS-diskette.
10. Typ achter de prompt **A:** `FORMAT C: /S` en druk op Enter. Format zorgt ervoor dat het USB-flashapparaat wordt geformatteerd, dat de systeembestanden worden toegevoegd en vraagt om een volumelabel.
11. Druk op Enter als u geen label wilt invoeren of voer een label in.
12. Zet de computer uit en haal het netsnoer uit het stopcontact. Open de computer en installeer de PCI-kaarten die eerder uit de computer werden verwijderd. Sluit de behuizing van de computer.
13. Stop de stekker in het stopcontact, verwijder de diskette en zet de computer weer aan.
14. Druk zodra de computer is ingeschakeld op de sneltoets F10, voordat het besturingssysteem wordt geladen, om Computer Setup (Computerinstellingen) te openen. Druk op Enter om een eventueel beginscherm over te slaan.

15. Ga naar **Advanced** (Geavanceerd) > **PCI Devices** (PCI-apparaten) en schakel de PATA- en SATA-controllers die u in stap 6 had uitgeschakeld weer in. Stel de oorspronkelijke IRQ weer in voor de SATA-controller.

16. Sla de wijzigingen op en sluit af. De computer wordt opgestart vanaf het USB-flashapparaat dat C als stationsletter krijgt.

OPMERKING: De standaardopstartvolgorde verschilt per computer en kan worden gewijzigd in Computer Setup (Computerinstellingen). Raadpleeg de *Handleiding Computerinstellingen* voor instructies.

Als u een DOS-versie van Windows 9x heeft gebruikt, krijgt u waarschijnlijk even een scherm met Windows-logo te zien. Als u dit scherm niet wilt, voegt u een leeg bestand, LOGO.SYS, toe aan de hoofddirectory van het USB-flashapparaat.

Ga terug naar Kopiëren naar meerdere computers op pagina 17.

8 Aan/uit-knop met twee standen

Als Advanced Configuration and Power Interface (ACPI) is ingeschakeld, kan de aan/uit-knop functioneren als aan/uit-schakelaar of als een standbyknop. In de standbystand wordt de stroomvoorziening niet helemaal afgesloten, maar verbruikt de computer minder energie. Hierdoor kunt u snel het stroomverbruik beperken zonder dat u applicaties hoeft te sluiten en kan de computer snel naar de oorspronkelijke stand terugkeren zonder dat u gegevens verliest.

Ga als volgt te werk om de configuratie van de aan/uit-knop te wijzigen:

1. Klik op **Start** selecteer vervolgens **Configuratiescherm** > **Energiebeheer**.
2. Selecteer het tabblad **Geavanceerd** in het venster **Eigenschappen voor Energiebeheer**.
3. Selecteer in het gedeelte **Aan/uit-knop** de optie **Standby**.

Als u de aan/uit-knop eenmaal heeft geconfigureerd als standbyknop, kunt u met deze knop overschakelen op een stand met een bijzonder laag energieverbruik. Druk nogmaals op deze knop om weer terug te gaan naar de maximale stroomvoorziening. Als u de stroomvoorziening helemaal wilt uitschakelen, houdt u de aan/uit-knop vier seconden ingedrukt.

△ **VOORZICHTIG:** Gebruik de aan/uit-knop niet om de computer uit te schakelen, tenzij het systeem niet meer reageert. Als u de stroomtoevoer uitschakelt zonder tussenkomst van het besturingssysteem, kunnen er gegevens op de vaste schijf beschadigd raken of verloren gaan.

9 HP ondersteuningswebsite

HP verzorgt grondige tests en debugprocedures van software die door HP of andere leveranciers wordt ontwikkeld. Bovendien ontwikkelt HP ondersteunende software specifiek voor elk besturingssysteem, zodat HP computers optimaal presteren op het gebied van snelheid, compatibiliteit en betrouwbaarheid.

Wanneer u overschakelt naar een ander besturingssysteem of naar een nieuwere versie van het besturingssysteem, is het belangrijk om de ondersteunende software te implementeren die is ontwikkeld voor het desbetreffende besturingssysteem of de desbetreffende versie. Als u een andere versie van Microsoft Windows wilt gebruiken dan de versie die bij de computer is geleverd, is het noodzakelijk dat u de overeenkomstige stuurprogramma's en hulpprogramma's installeert, zodat alle voorzieningen worden ondersteund en naar behoren functioneren.

HP heeft het vinden, openen, evalueren en installeren van de recentste ondersteuningssoftware eenvoudiger gemaakt. U kunt de software downloaden vanaf http://www.hp.com/support.

De website bevat de meest recente versie van stuurprogramma's, hulpprogramma's en flash-ROM-images die nodig zijn om het meest recente Microsoft Windows-besturingssysteem op de HP computer uit te voeren.

10 Industriestandaarden

De HP oplossingen voor systeembeheer kunnen goed worden geïntegreerd met andere applicaties voor systeembeheer en zijn gebaseerd op industriestandaarden, zoals:

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

11 Inventarisbeheer en beveiliging

Ingebouwde functies voor inventarisbeheer leveren essentiële inventarisgegevens op, die kunnen worden beheerd met HP Systems Insight Manager, HP Client Manager, HP Configuration Management Solution, HP Client Configuration Manager of andere applicaties voor systeembeheer. Dankzij de naadloze, automatische integratie van de voorzieningen voor inventarisbeheer met deze producten, kunt u een hulpprogramma voor computerbeheer kiezen dat het beste aansluit op uw omgeving, zodat uw investering in bestaande software zijn waarde behoudt.

HP biedt ook mogelijkheden om de toegang tot waardevolle onderdelen en informatie te beveiligen. Als HP Embedded Security for ProtectTools is geïnstalleerd, wordt onbevoegde toegang tot gegevens voorkomen, de integriteit van het systeem gecontroleerd en worden derden die het systeem proberen te gebruiken, eerst geverifieerd. (Raadpleeg voor meer informatie de *HP ProtectTools Security Manager Guide* (Handleiding HP ProtectTools Security Manager) op http://www.hp.com/products/security.) Met behulp van beveiligingsvoorzieningen als HP Embedded Security for ProtectTools, Smart Cover Sensor en Smart Cover Lock, die op bepaalde modellen beschikbaar zijn, kunt u onbevoegde toegang tot de interne onderdelen van de computer voorkomen. Door parallelle poorten, seriële poorten of USB-poorten uit te schakelen of door het onmogelijk te maken om de computer op te starten vanaf een verwisselbare schijfeenheid, kunt u waardevolle gegevens beschermen. Waarschuwingen bij geheugenwijzigingen en waarschuwingen van de Smart Cover Sensor kunnen automatisch worden doorgestuurd naar applicaties voor systeembeheer, zodat geknoei met de interne onderdelen van een computer vroegtijdig wordt gemeld.

OPMERKING: HP Embedded Security for ProtectTools, Smart Cover Sensor en Smart Cover Lock, zijn op bepaalde systemen als optie beschikbaar.

Er zijn verschillende manieren waarop beveiligingsinstellingen op HP computers kunnen worden beheerd:

- Lokaal, met behulp van de hulpprogramma's in Computer Setup (Computerinstellingen). Raadpleeg de *Handleiding Computerinstellingen* die is meegeleverd bij de computer voor aanvullende informatie en instructies over het gebruik van Computer Setup (Computerinstellingen).
- Op afstand, met HP Client Manager from Symantec, HP Client Automation of System Software Manager. Hiermee kunt u software op een veilige en consistente manier implementeren en de beveiligingsinstellingen controleren.

In de volgende tabel en gedeelten vindt u informatie over het lokale beheer van beveiligingsvoorzieningen op de computer via het hulpprogramma Computer Setup (Computerinstellingen).

Tabel 11-1 Overzicht van beveiligingsvoorzieningen

Optie	Beschrijving
Setup Password (Instelwachtwoord)	Hiermee kunt u een instelwachtwoord (beheerderswachtwoord) definiëren en inschakelen.

Tabel 11-1 Overzicht van beveiligingsvoorzieningen (vervolg)

	OPMERKING: Als het instelwachtwoord is gedefinieerd, heeft u dit wachtwoord nodig om wijzigingen aan te brengen in de opties van Computer Setup, om een ROM-flash uit te voeren en om wijzigingen aan te brengen in bepaalde Plug and play-instellingen van Windows.
Power-On Password (Opstartwachtwoord)	Hiermee kunt u een opstartwachtwoord instellen en inschakelen. De gebruikers wordt telkens naar het opstartwachtwoord gevraagd nadat het systeem is uit- en weer aangezet. Als de gebruiker niet het juiste opstartwachtwoord geeft, zal het systeem niet opstarten. **OPMERKING:** Het wachtwoord wordt niet gevraagd bij een warme start, bijvoorbeeld met Ctrl + Alt + Delete of **Restart from Windows** (Opnieuw opstarten vanuit Windows), tenzij dat hieronder is ingeschakeld bij **Password Options** (Wachtwoordopties).
Password Options (Wachtwoordopties) (Deze selectie wordt alleen weergegeven als er een opstart- of instelwachtwoord is ingesteld.)	Hiermee kunt u het volgende doen: • Oudere bronnen vergrendelen (wordt weergegeven als een instelwachtwoord is ingesteld). • Netwerkservermodus in- of uitschakelen (wordt weergegeven als een opstartwachtwoord is ingesteld). • Aangeven of het wachtwoord is vereist voor warm opstarten (Ctrl+Alt+Delete) (wordt weergegeven als een opstartwachtwoord is ingesteld). • Setup Browse Mode (Bladermodus voor Computerinstellingen) in- of uitschakelen (wordt weergegeven als een instelwachtwoord is ingesteld) (zorgt ervoor dat de opties voor Computer Setup kunnen worden bekeken, maar niet worden gewijzigd, zonder dat een instelwachtwoord hoeft te worden opgegeven). • Enable/disable Stringent Password (Strenge wachtwoordbeveiliging inschakelen/uitschakelen, wordt weergegeven wanneer een opstartwachtwoord wordt ingesteld). Wanneer deze optie is ingeschakeld, wordt de onboard wachtwoordjumper genegeerd om het opstartwachtwoord uit te schakelen. Raadpleeg de handleiding *Desktop Management* voor meer informatie.
Smart Cover (intelligente vergrendeling, op bepaalde modellen)	Hiermee kunt u het volgende doen: • Cover Lock (kapvergrendeling) vergrendelen en ontgrendelen. • Cover Removal Sensor (sensor voor verwijdering van de computerkap) instellen op Disable (Uitschakelen), Notify User (Gebruiker waarschuwen) of Setup Password (Instelwachtwoord). **OPMERKING:** Als *Notify User* (Gebruiker waarschuwen) is ingeschakeld, wordt de gebruiker gewaarschuwd wanneer de sensor heeft gedetecteerd dat de kap is verwijderd. Als *Setup Password* (Instelwachtwoord) is ingeschakeld, moet het instelwachtwoord worden ingevoerd om de computer op te starten wanneer de sensor vaststelt dat de kap is verwijderd. Deze optie is alleen voor bepaalde modellen beschikbaar.
Device Security (Beveiliging apparatuur)	Hiermee kunt u Device Available/Device Hidden (Apparaat beschikbaar/apparaat verbergen) instellen voor: • seriële poorten • parallelle poort • USB-poorten aan de achterzijde • USB-poorten aan de voorzijde • interne USB-poorten • systeemaudio • netwerkadapters (bepaalde modellen) • Legacy Diskette (Oudere diskette):

Tabel 11-1 Overzicht van beveiligingsvoorzieningen (vervolg)

	• ingebouwd beveiligingsapparaat (bepaalde modellen) • SATA0 • SATA1 (bepaalde modellen) • SATA2 (bepaalde modellen) • SATA3 (bepaalde modellen) • eSATA (bepaalde modellen)
LoJack for HP ProtectTools	Hiermee kunt u de computer op afstand bewaken, beheren en volgen. Nadat LoJack Pro for HP ProtectTools is geactiveerd, wordt het geconfigureerd vanuit het Absolute Software Customer Center. Vanuit het Customer Center kan de beheerder LoJack for HP ProtectTools configureren voor het bewaken en beheren van de computer. Als de computer kwijt is of wordt gestolen, kan het Customer Center lokale instanties ondersteunen bij het vinden en herstellen van de computer. Nadat LoJack Pro is geconfigureerd, kan het ook blijven functioneren wanneer de vaste schijf wordt gewist of vervangen.
Network Service Boot (Opstarten via netwerkservice)	Hiermee schakelt u de mogelijkheid in of uit om de computer op te starten vanaf een besturingssysteem dat op een netwerkserver is geïnstalleerd. (Deze optie is alleen beschikbaar voor modellen met een netwerkadapter. De netwerkkaart moet in dit geval een PCI-uitbreidingskaart zijn of in de systeemkaart zijn geïntegreerd.)
System IDs (Systeemidentificatie)	Hiermee kunt u het volgende instellen: • Inventarisnummer (18-byte code), eigendomsidentificatienummer dat het bedrijf heeft toegekend aan deze computer. • Eigendomslabel (80-byte code) dat wordt weergegeven tijdens POST. • Serienummer van het chassis of het UUID-nummer (Universal Unique Identifier). Het UUID-nummer kan alleen worden gewijzigd als het huidige serienummer van het chassis ongeldig is. (Deze identificatienummers worden normaal gesproken in de fabriek ingesteld en dienen ter eenduidige identificatie van het systeem.) • De toetsenbordinstelling (in Nederland wordt meestal de instelling VS/Internationaal gebruikt).
DriveLock Security (DriveLock-beveiliging)	Hiermee kunt u een hoofd- of gebruikerswachtwoord toewijzen aan, of wijzigen voor, vaste schijven. Als deze functie is ingeschakeld, moet een van de DriveLock-wachtwoorden worden ingevoerd tijdens de POST. Als geen van beide wachtwoorden wordt ingevoerd, is de vaste schijf niet toegankelijk tot een van de wachtwoorden wordt ingevoerd tijdens de volgende koude start. **OPMERKING:** Deze keuzemogelijkheid verschijnt alleen als ten minste één schijfeenheid die DriveLock ondersteunt, is aangesloten op het systeem.

Tabel 11-1 Overzicht van beveiligingsvoorzieningen (vervolg)

Setup Security Level (Niveau van configuratiebeveiliging)	Met deze optie kunt u eindgebruikers beperkte toegang tot bepaalde configuratieopties geven, zonder dat zij het instelwachtwoord hoeven te kennen. Hiermee beschikken beheerders over de flexibiliteit om essentiële configuratieopties te beschermen tegen wijzigingen, terwijl zij gebruikers wel de mogelijkheid kunnen bieden systeeminstellingen te bekijken en minder essentiële opties te configureren. De beheerder stelt voor elke afzonderlijke configuratieoptie toegangsrechten in via het menu Setup Security Level (Niveau van configuratiebeveiliging). Standaard wordt aan alle configuratieopties het instelwachtwoord toegewezen, zodat de gebruiker tijdens de zelftest (POST) het juiste instelwachtwoord moet opgeven om wijzigingen in een optie te kunnen aanbrengen. De beheerder kan bepaalde items instellen op None (Geen), zodat de gebruiker de desbetreffende opties kan wijzigen wanneer Computer Setup is geopend met een ongeldig wachtwoord. De optie None (Geen) wordt vervangen door Power-On Password (Opstartwachtwoord) als een opstartwachtwoord is ingesteld. **OPMERKING:** Als de gebruiker Computer Setup wil openen terwijl deze het instelwachtwoord niet kent, moet Setup Browse Mode (Bladermodus voor Computer Setup) zijn ingesteld op Enable (Inschakelen).
OS Security (Beveiliging besturingssysteem) (bepaalde modellen; deze opties zijn afhankelijk van de hardware)	Data Execution Prevention (enable/disable) (Voorkomen van gegevensuitvoering (in-/uitschakelen), bepaalde modellen): hiermee kunt u schending van de beveiliging van het besturingssysteem voorkomen. Virtualization Technology (enable/disable) (Technologie voor virtuele netwerken (in-/uitschakelen), bepaalde modellen): hiermee controleert u de virtualisatievoorzieningen van de processor. Nadat deze instelling is gewijzigd, moet de computer worden uitgeschakeld en weer ingeschakeld. Virtualization Technology Directed I/O (enable/disable) (I/O doorgeleid door technologie voor virtuele netwerken (in-/uitschakelen), bepaalde modellen): hiermee controleert u de DMA-hertoewijzingsfuncties voor virtualisatievoorzieningen van de chipset. Nadat deze instelling is gewijzigd, moet de computer worden uitgeschakeld en weer ingeschakeld. Trusted Execution Technology (enable/disable) (Technologie voor vertrouwde uitvoering (in-/uitschakelen), bepaalde modellen): hiermee controleert u de onderliggende functies van de processor en chipset die nodig zijn om een virtueel apparaat te ondersteunen. Nadat deze instelling is gewijzigd, moet de computer worden uitgeschakeld en weer ingeschakeld. Als u deze voorziening wilt inschakelen, moeten eerst de volgende voorzieningen worden ingeschakeld: • Embedded Security Device Support (Ondersteuning voor geïntegreerd beveiligingsapparaat) • Virtualization Technology (Technologie voor virtuele netwerken) • Virtualization Technology Directed I/O (I/O doorgeleid door technologie voor virtuele netwerken) Embedded Security Device Support (enable/disable) (Ondersteuning voor geïntegreerd beveiligingsapparaat (inschakelen/uitschakelen), bepaalde modellen): hiermee kan het geïntegreerde beveiligingsapparaat worden in- of uitgeschakeld. Nadat deze instelling is gewijzigd, moet de computer worden uitgeschakeld en weer ingeschakeld. **OPMERKING:** Voor het configureren van een geïntegreerd beveiligingsapparaat moet een instelwachtwoord worden ingesteld. • Reset to Factory Settings (Do not reset/Reset) (Fabrieksinstellingen herstellen (niet herstellen/herstellen), bepaalde modellen): wanneer u de standaard fabrieksinstellingen herstelt, worden alle beveiligingssleutels gewist. Nadat deze instelling is gewijzigd, moet de computer worden uitgeschakeld en weer ingeschakeld. **VOORZICHTIG:** Het geïntegreerde beveiligingsapparaat is een cruciaal onderdeel van veel beveiligingsschema's. Wanneer de beveiligingssleutels worden gewist, zijn gegevens die door het geïntegreerde beveiligingsapparaat worden beveiligd niet meer toegankelijk. Als u Reset to Factory Settings (Fabrieksinstellingen herstellen) kiest, kunnen belangrijke gegevens verloren gaan. • Reset authentication credentials (Do not reset/Reset) (Verificatiereferenties herstellen (niet herstellen/herstellen), bepaalde modellen): nadat deze instelling is gewijzigd, moet de computer worden uitgeschakeld en weer ingeschakeld.

Tabel 11-1 Overzicht van beveiligingsvoorzieningen (vervolg)

	OS Management of Embedded Security Device (enable/disable) (Beheer door besturingssysteem van geïntegreerd beveiligingsapparaat (inschakelen/uitschakelen), bepaalde modellen): hiermee kan de gebruiker het beheer van het geïntegreerde beveiligingsapparaat door het besturingssysteem in- of uitschakelen. Nadat deze instelling is gewijzigd, moet de computer worden uitgeschakeld en weer ingeschakeld. Via deze optie kan de gebruiker het beheer van het geïntegreerde beveiligingsapparaat door het besturingssysteem beperken. • Reset of Embedded Security Device through OS (enable/disable) (Geïntegreerd beveiligingsapparaat herstellen door het besturingssysteem (inschakelen/uitschakelen), bepaalde modellen): hiermee kan de gebruiker de mogelijkheid beperken dat het besturingssysteem het geïntegreerde beveiligingsapparaat verzoekt de fabrieksinstellingen te herstellen. Nadat deze instelling is gewijzigd, moet de computer worden uitgeschakeld en weer ingeschakeld. **OPMERKING:** Deze optie kan alleen worden ingeschakeld als er een instelwachtwoord is ingesteld. PAVP (disabled/min/max) (PAVP (uitgeschakeld/min/max), bepaalde modellen): PAVP schakelt de Protected Audio Video Path in de chipset in. Dit zorgt ervoor dat bepaalde beveiligde high-definition content kan worden bekeken die normaalgesproken niet kan worden afgespeeld. Als u de instelling Max selecteert, wordt 96 MB systeemgeheugen exclusief toegewezen aan PAVP.

Wachtwoordbeveiliging

Het opstartwachtwoord voorkomt dat onbevoegden de computer kunnen gebruiken. Telkens wanneer een gebruiker de computer inschakelt of opnieuw opstart, moet deze een wachtwoord invoeren om toegang te krijgen tot applicaties of gegevens. Het instelwachtwoord voorkomt specifiek onbevoegde toegang tot Computer Setup (Computerinstellingen) en kan ook worden gebruikt in plaats van het opstartwachtwoord. Dit betekent dat als u het instelwachtwoord invoert wanneer om het opstartwachtwoord wordt gevraagd, u toch toegang krijgt tot de computer.

Er kan een voor het hele netwerk geldig instelwachtwoord worden ingesteld om de systeembeheerder in staat te stellen zich aan te melden op alle netwerksystemen om onderhoud uit te voeren, zonder het opstartwachtwoord te hoeven kennen, ook al is er een ingesteld.

OPMERKING: System Software Manager (SSM) kan worden gebruikt om BIOS-wachtwoorden te maken en beheren vanuit het besturingssysteem Windows. Raadpleeg voor meer informatie de gebruikershandleiding van SSM op http://www.hp.com/go/ssm.

OPMERKING: HP Client Management Interface (HP CMI) biedt toegang tot het BIOS-instellingenbeheer, inclusief BIOS-wachtwoorden, vanuit het besturingssysteem Windows. Raadpleeg voor meer informatie het HP Client Management Interface Technical Whitepaper op http://www.hp.com/go/hpcmi.

Instelwachtwoord definiëren met Computer Setup

Als het systeem is voorzien van een apparaat voor geïntegreerde beveiliging, raadpleegt u de handleiding *HP ProtectTools Security Manager* op http://www.hp.com. Door een instelwachtwoord te

definiëren in Computer Setup (Computerinstellingen), voorkomt u dat de computer opnieuw wordt geconfigureerd (via Computer Setup) totdat het wachtwoord wordt ingevoerd.

1. Schakel de computer in of start de computer opnieuw op. Selecteer hiervoor in Windows **Start** > **Uitschakelen** > **Opnieuw opstarten**.
2. Druk zodra de computer is ingeschakeld op de sneltoets F10, voordat het besturingssysteem wordt geladen, om Computer Setup (Computerinstellingen) te openen. Druk op Enter om een eventueel beginscherm over te slaan.

OPMERKING: Als u niet op het juiste moment op F10 drukt, start u de computer opnieuw op en drukt u op F10 voordat het besturingssysteem wordt geladen, om het hulpprogramma te openen.

3. Selecteer achtereenvolgens **Security** (Beveiliging) en **Setup Password** (Instelwachtwoord) en volg de instructies op het scherm.
4. Selecteer achtereenvolgens **File** (Bestand) > **Save Changes and Exit** (Wijzigingen opslaan en afsluiten).

Opstartwachtwoord definiëren met Computer Setup

Het opstartwachtwoord is een beveiligingsvoorziening waarmee de computer alleen kan worden gebruikt als eerst een wachtwoord wordt ingevoerd. Als u een opstartwachtwoord heeft ingesteld, verschijnt de opdracht **Password Options** (Wachtwoordopties) in het menu **Security** (Beveiliging). Een van de wachtwoordopties is **Password Prompt on Warm Boot** (Wachtwoordprompt bij warme start). Als deze optie is ingeschakeld, moet u het wachtwoord ook invoeren telkens wanneer u de computer opnieuw opstart.

1. Zet de computer aan of start de computer opnieuw op. Selecteer hiervoor in Windows **Start** > **Uitschakelen** > **Opnieuw opstarten**.
2. Druk zodra de computer is ingeschakeld op de sneltoets F10, voordat het besturingssysteem wordt geladen, om Computer Setup (Computerinstellingen) te openen. Druk op Enter om een eventueel beginscherm over te slaan.

OPMERKING: Als u niet op het juiste moment op F10 drukt, start u de computer opnieuw op en drukt u op F10 voordat het besturingssysteem wordt geladen, om het hulpprogramma te openen.

3. Selecteer achtereenvolgens **Security** (Beveiliging) en **Power-On Password** (Opstartwachtwoord) en volg de instructies op het scherm.
4. Selecteer achtereenvolgens **File** (Bestand) > **Save Changes and Exit** (Wijzigingen opslaan en afsluiten).

Opstartwachtwoord invoeren

Ga als volgt te werk om een opstartwachtwoord in te voeren:

1. Schakel de computer in of start de computer opnieuw op. Selecteer hiervoor in Windows **Start** > **Afsluiten** > **Computer opnieuw opstarten**.
2. Wanneer het sleutelpictogram op het beeldscherm verschijnt, typt u het huidige wachtwoord en drukt u op Enter.

OPMERKING: Typ zorgvuldig. Uit veiligheidsoverwegingen worden de tekens die u typt niet op het scherm weergegeven.

Als u het wachtwoord verkeerd invoert, verschijnt het pictogram van een gebroken sleutel. Probeer het opnieuw. Na drie mislukte pogingen moet u de computer uitzetten en opnieuw opstarten voordat u verder kunt.

Instelwachtwoord invoeren

Als het systeem is voorzien van een apparaat voor geïntegreerde beveiliging, raadpleegt u de handleiding *HP ProtectTools Security Manager* op http://www.hp.com.

Als een instelwachtwoord op de computer is gedefinieerd, wordt u gevraagd dit in te voeren wanneer u Computer Setup (Computerinstellingen) wilt uitvoeren.

1. Schakel de computer in of start de computer opnieuw op. Selecteer hiervoor in Windows **Start** > **Uitschakelen** > **Opnieuw opstarten**.
2. Druk zodra de computer is ingeschakeld op de sneltoets F10, voordat het besturingssysteem wordt geladen, om Computer Setup (Computerinstellingen) te openen. Druk op Enter om een eventueel beginscherm over te slaan.

OPMERKING: Als u niet op het juiste moment op F10 drukt, start u de computer opnieuw op en drukt u op F10 voordat het besturingssysteem wordt geladen, om het hulpprogramma te openen.

3. Wanneer het sleutelpictogram op het beeldscherm verschijnt, typt u het instelwachtwoord en drukt u op Enter.

OPMERKING: Typ zorgvuldig. Uit veiligheidsoverwegingen worden de tekens die u typt niet op het scherm weergegeven.

Als u het wachtwoord verkeerd invoert, verschijnt het pictogram van een gebroken sleutel. Probeer het opnieuw. Na drie mislukte pogingen moet u de computer uitzetten en opnieuw opstarten voordat u verder kunt.

Opstart- of instelwachtwoord wijzigen

Als het systeem is voorzien van een apparaat voor geïntegreerde beveiliging, raadpleegt u de handleiding *HP ProtectTools Security Manager* op http://www.hp.com.

1. Schakel de computer in of start de computer opnieuw op. Selecteer hiervoor in Windows **Start** > **Afsluiten** > **Computer opnieuw opstarten**.
2. Ga naar stap 3 als u het opstartwachtwoord wilt wijzigen.

   Als u het instelwachtwoord wilt wijzigen, drukt u zodra de computer is ingeschakeld op de sneltoets F10, voordat het besturingssysteem wordt geladen, om Computer Setup (Computerinstellingen) te openen. Druk op Enter om een eventueel beginscherm over te slaan.

OPMERKING: Als u niet op het juiste moment op F10 drukt, start u de computer opnieuw op en drukt u op F10 voordat het besturingssysteem wordt geladen, om het hulpprogramma te openen.

3. Voer als het sleutelpictogram verschijnt het huidige wachtwoord in, gevolgd door een schuine streep (/) of een ander scheidingsteken, het nieuwe wachtwoord, nog een schuine streep (/) of een ander scheidingsteken en tot slot nogmaals het nieuwe wachtwoord: `huidig wachtwoord/nieuw wachtwoord/nieuw wachtwoord`

OPMERKING: Typ zorgvuldig. Uit veiligheidsoverwegingen worden de tekens die u typt niet op het scherm weergegeven.

4. Druk op Enter.

Het nieuwe wachtwoord wordt van kracht als u de computer opnieuw aanzet.

OPMERKING: Raadpleeg Scheidingstekens en land-/regiospecifieke toetsenborden op pagina 32 voor informatie over alternatieve scheidingstekens. Het opstartwachtwoord en het instelwachtwoord kunnen ook worden gewijzigd met behulp van de beveiligingsopties in Computer Setup.

Opstart- of instelwachtwoord verwijderen

Als het systeem is voorzien van een apparaat voor geïntegreerde beveiliging, raadpleegt u de handleiding *HP ProtectTools Security Manager* op http://www.hp.com.

1. Schakel de computer in of start de computer opnieuw op. Selecteer hiervoor in Windows **Start** > **Afsluiten** > **Computer opnieuw opstarten**.
2. Ga naar stap 3 als u het opstartwachtwoord wilt verwijderen.

   Als u het instelwachtwoord wilt wissen, drukt u zodra de computer is ingeschakeld op de sneltoets F10, voordat het besturingssysteem wordt geladen, om Computer Setup (Computerinstellingen) te openen. Druk op Enter om een eventueel beginscherm over te slaan.

   OPMERKING: Als u niet op het juiste moment op F10 drukt, start u de computer opnieuw op en drukt u op F10 voordat het besturingssysteem wordt geladen, om het hulpprogramma te openen.
3. Voer als het sleutelpictogram verschijnt het huidige wachtwoord in, gevolgd door een schuine streep (/) of een ander scheidingsteken: `huidig wachtwoord/`
4. Druk op Enter.

   OPMERKING: Raadpleeg Scheidingstekens en land-/regiospecifieke toetsenborden op pagina 32 voor informatie over alternatieve scheidingstekens. Het opstartwachtwoord en het instelwachtwoord kunnen ook worden gewijzigd met behulp van de beveiligingsopties in Computer Setup.

Scheidingstekens en land-/regiospecifieke toetsenborden

Elk toetsenbord is ontworpen om tegemoet te komen aan land-/regiospecifieke vereisten. De syntax en de toetsen die u gebruikt om een wachtwoord te wijzigen of te verwijderen, zijn afhankelijk van het toetsenbord dat bij de computer is geleverd. In Nederland wordt meestal gebruik gemaakt van het toetsenbord VS/Internationaal.

Scheidingstekens en land-/regiospecifieke toetsenborden					
/	Arabisch	-	Grieks	/	Russisch
=	Belgisch	.	Hebreeuws	-	Slowaaks
-	BHKMSS*	-	Hongaars	-	Spaans
/	Braziliaans	-	Italiaans	/	Zweeds/Fins
/	Chinees	/	Japans	-	Zwitsers
-	Tsjechisch	/	Koreaans	/	Taiwanees
-	Deens	-	Latijns-Amerikaans	/	Thais
!	Frans	-	Noors	.	Turks
é	Canadees (Frans)	-	Pools	/	VS/Internationaal

Scheidingstekens en land-/regiospecifieke toetsenborden	
- Duits	- Portugees
* Voor Bosnië-Herzegovina, Kroatië, Montenegro, Servië en Slovenië	

Wachtwoorden wissen

Als u het wachtwoord bent vergeten, heeft u geen toegang tot de computer. Raadpleeg de handleiding *Problemen oplossen* voor instructies over het wissen van wachtwoorden.

Als het systeem is voorzien van een apparaat voor geïntegreerde beveiliging, raadpleegt u de handleiding *HP ProtectTools Security Manager* op http://www.hp.com.

DriveLock

DriveLock is een beveiligingsvoorziening die onbevoegde toegang tot gegevens op vaste schijven van het type ATA voorkomt. DriveLock is geïmplementeerd als een uitbreiding van Computer Setup (Computerinstellingen). Deze functie is uitsluitend beschikbaar wanneer vaste schijven die de ATA Security-opdrachten ondersteunen, worden gedetecteerd. DriveLock is bedoeld voor gebruikers van HP systemen voor wie gegevensbeveiliging van het allergrootste belang is. Voor deze gebruikers zijn de kosten van de vaste schijf en het verlies van de gegevens op de schijf irrelevant vergeleken bij de schade die het gevolg kan zijn van onbevoegde toegang tot de inhoud van de schijf. De HP implementatie van DriveLock maakt gebruik van een beveiligingsschema met twee wachtwoorden om dit beveiligingsniveau toe te kunnen passen, maar tegelijkertijd rekening te houden met de mogelijkheid dat een wachtwoord wordt vergeten. Het ene wachtwoord wordt ingesteld en gebruikt door de systeembeheerder, het andere wordt doorgaans ingesteld en gebruikt door de eindgebruiker. Er is geen "achterdeur": als u beide wachtwoorden vergeet, kan de schijfeenheid niet meer worden ontgrendeld. Daarom wordt u aangeraden de gegevens op de vaste schijf te kopiëren naar een bedrijfsinformatiesysteem of er regelmatig een back-up van te maken. Als u beide DriveLock-wachtwoorden vergeet, kan de vaste schijf niet meer worden gebruikt. Voor gebruikers die niet beantwoorden aan het hierboven gedefinieerde profiel, is dit wellicht een onacceptabel risico. Voor gebruikers die wel beantwoorden aan dit profiel, is dit risico mogelijk acceptabel vanwege het type gegevens op de vaste schijf.

DriveLock gebruiken

Wanneer een of meerdere vaste schijven die de ATA Security-opdrachten ondersteunen, worden gedetecteerd, wordt de optie DriveLock weergegeven in het menu Security (Beveiliging) in Computer Setup (Computerinstellingen). U kunt kiezen uit opties om het hoofdwachtwoord in te stellen of DriveLock in te schakelen. Om DriveLock te kunnen inschakelen, moet een gebruikerswachtwoord worden opgeven. Aangezien de initiële configuratie van DriveLock doorgaans wordt uitgevoerd door de systeembeheerder, stelt u wellicht eerst een hoofdwachtwoord in. De systeembeheerder wordt aangeraden altijd een hoofdwachtwoord in te stellen, ongeacht of DriveLock wordt ingeschakeld. Hierdoor kan de systeembeheerder de instellingen van DriveLock wijzigen als de schijfeenheid in de toekomst wordt vergrendeld. Nadat het hoofdwachtwoord is ingesteld, kan de systeembeheerder desgewenst DriveLock inschakelen.

Als het systeem een vergrendelde vaste schijf bevat, wordt u tijdens POST gevraagd een wachtwoord in te voeren om de schijf te ontgrendelen. Als een opstartwachtwoord is ingesteld en dit overeenkomt met het gebruikerswachtwoord voor de schijf, wordt u niet gevraagd het wachtwoord nogmaals in te voeren. Als twee verschillende wachtwoorden worden gebruikt, wordt u wel gevraagd een DriveLock-wachtwoord in te voeren. Bij een koude start kunt u hiervoor het hoofdwachtwoord of het

gebruikerswachtwoord gebruiken. Bij een warme start gebruikt u hetzelfde wachtwoord dat u heeft gebruikt om de schijf te ontgrendelen bij de voorgaande koude start. U mag één keer een verkeerd wachtwoord invoeren. Als u bij een koude start twee keer een verkeerd wachtwoord invoert, wordt POST verder uitgevoerd maar heeft u geen toegang tot de schijf. Als bij een warme start of bij het opnieuw opstarten vanuit Windows geen enkele poging lukt, stopt POST en wordt de gebruiker gevraagd de computer uit- en direct weer in te schakelen.

DriveLock applicaties

De meest praktische toepassing van de DriveLock-beveiligingsvoorziening is in een bedrijfsomgeving. De systeembeheerder is doorgaans verantwoordelijk voor het configureren van de vaste schijf. Dit houdt onder andere in het instellen van het DriveLock-hoofdwachtwoord en een tijdelijk gebruikerswachtwoord. Als een gebruiker het gebruikerswachtwoord vergeet of de apparatuur door een andere werknemer wordt gebruikt, kan het hoofdwachtwoord worden gebruikt om het gebruikerswachtwoord opnieuw in te stellen, zodat de gegevens op de vaste schijf opnieuw toegankelijk worden.

Systeembeheerders van bedrijven die DriveLock willen gebruiken, wordt aangeraden ook een bedrijfsbeleid in te stellen voor het instellen en bijhouden van hoofdwachtwoorden, om te voorkomen dat een werknemer met opzet of per ongeluk beide DriveLock-wachtwoorden wijzigt voordat hij of zij het bedrijf verlaat. In dat geval zou de vaste schijf onbruikbaar zijn en moeten worden vervangen. Als de systeembeheerder geen hoofdwachtwoord instelt, is het ook mogelijk dat de beheerder geen toegang meer heeft tot een vaste schijf en geen routinecontroles kan uitvoeren op ongeoorloofde software, andere functies voor inventarisbeheer en ondersteuning.

Als u minder strikte beveiligingsvereisten heeft, wordt u afgeraden DriveLock in te schakelen. Dit geldt voor privégebruikers of gebruikers die doorgaans geen vertrouwelijke gegevens op hun vaste schijf hebben. Voor deze gebruikers is het mogelijke verlies van een vaste schijf wanneer beide wachtwoorden zijn vergeten, van veel groter belang dan de waarde van de gegevens die door DriveLock worden beveiligd. Gebruik het instelwachtwoord om de toegang tot Computer Setup (Computerinstellingen) en DriveLock te beperken. Door een instelwachtwoord op te geven maar dit niet aan de eindgebruiker mee te delen, kan de systeembeheerder voorkomen dat andere gebruikers DriveLock inschakelen.

Smart Cover Sensor

Cover Removal Sensor (alleen bepaalde modellen) is een combinatie van hardware- en softwaretechnologie die u kan waarschuwen wanneer de afdekplaat of het zijpaneel van de computer wordt verwijderd. Er zijn drie beschikbare beveiligingsniveaus, die worden beschreven in de volgende tabel.

Tabel 11-2 Smart Cover Sensor - beveiligingsniveaus

Niveau	Instelling	Beschrijving
Niveau 0	Disabled (Uitgeschakeld)	De Smart Cover Sensor is uitgeschakeld (standaardinstelling).
Niveau 1	Notify User (Gebruiker waarschuwen)	Bij het opnieuw starten van de computer verschijnt de mededeling dat de kap of het zijpaneel van de computer is verwijderd.
Niveau 2	Setup Password (Instelwachtwoord)	Bij het opnieuw starten van de computer verschijnt de mededeling dat de kap of het zijpaneel van de computer is verwijderd. Voer het instelwachtwoord om door te gaan.

OPMERKING: Deze instellingen kunnen worden gewijzigd met behulp van Computer Setup (Computerinstellingen). Raadpleeg de *Handleiding Computerinstellingen* voor meer informatie over Computer Setup (Computerinstellingen).

Beveiligingsniveau Smart Cover Sensor instellen

Ga als volgt te werk om het beveiligingsniveau van de Smart Cover Sensor in te stellen:

1. Schakel de computer in of start de computer opnieuw op. Selecteer hiervoor in Windows **Start** > **Uitschakelen** > **Opnieuw opstarten**.
2. Druk zodra de computer is ingeschakeld op de sneltoets F10, voordat het besturingssysteem wordt geladen, om Computer Setup (Computerinstellingen) te openen. Druk op Enter om een eventueel beginscherm over te slaan.

   OPMERKING: Als u niet op het juiste moment op F10 drukt, start u de computer opnieuw op en drukt u op F10 voordat het besturingssysteem wordt geladen, om het hulpprogramma te openen.
3. Kies **Security** (Beveiliging) > **Smart Cover** (Intelligente vergrendeling) > **Cover Removal Sensor** (Kapsensor) en selecteer het gewenste beveiligingsniveau.
4. Selecteer achtereenvolgens **File** (Bestand) > **Save Changes and Exit** (Wijzigingen opslaan en afsluiten).

Smart Cover Lock

Smart Cover Lock is een softwarematige kapbeveiliging waarmee sommige HP pc's zijn uitgerust. Hiermee wordt voorkomen dat onbevoegden toegang krijgen tot de interne onderdelen. Bij levering van de computer is Smart Cover Lock niet vergrendeld.

△ **VOORZICHTIG:** Zorg ervoor dat u een instelwachtwoord definieert om de computerkap optimaal te beveiligen. Met het instelwachtwoord wordt ongeautoriseerde toegang tot het hulpprogramma Computer Setup (Computerinstellingen) voorkomen.

OPMERKING: Smart Cover Lock is op bepaalde modellen als optie leverbaar.

Smart Cover Lock vergrendelen

Ga als volgt te werk om Smart Cover Lock te activeren en vergrendelen:

1. Schakel de computer in of start de computer opnieuw op. Selecteer hiervoor in Windows **Start** > **Uitschakelen** > **Opnieuw opstarten**.
2. Druk zodra de computer is ingeschakeld op de sneltoets F10, voordat het besturingssysteem wordt geladen, om Computer Setup (Computerinstellingen) te openen. Druk op Enter om een eventueel beginscherm over te slaan.

   OPMERKING: Als u niet op het juiste moment op F10 drukt, start u de computer opnieuw op en drukt u op F10 voordat het besturingssysteem wordt geladen, om het hulpprogramma te openen.
3. Selecteer achtereenvolgens **Security** (Beveiliging) > **Smart Cover** (Intelligente vergrendeling) > **Cover Lock** (Kapvergrendeling) > **Lock** (Vergrendelen).
4. Selecteer achtereenvolgens **File** (Bestand) > **Save Changes and Exit** (Wijzigingen opslaan en afsluiten).

Smart Cover Lock ontgrendelen

1. Schakel de computer in of start de computer opnieuw op. Selecteer hiervoor in Windows **Start** > **Uitschakelen** > **Opnieuw opstarten**.
2. Druk zodra de computer is ingeschakeld op de sneltoets F10, voordat het besturingssysteem wordt geladen, om Computer Setup (Computerinstellingen) te openen. Druk op Enter om een eventueel beginscherm over te slaan.

   OPMERKING: Als u niet op het juiste moment op F10 drukt, start u de computer opnieuw op en drukt u op F10 voordat het besturingssysteem wordt geladen, om het hulpprogramma te openen.
3. Selecteer achtereenvolgens **Security** (Beveiliging) > **Smart Cover** (Intelligente vergrendeling) > **Cover Lock** (Kapvergrendeling) > **Unlock** (Ontgrendelen).
4. Selecteer achtereenvolgens **File** (Bestand) > **Save Changes and Exit** (Wijzigingen opslaan en afsluiten).

Smart Cover FailSafe-sleutel gebruiken

Als u Smart Cover Lock heeft ingeschakeld, maar het wachtwoord niet kunt invoeren om de beveiliging uit te schakelen, heeft u een Smart Cover FailSafe-sleutel nodig om de kap van de computer te openen. U gebruikt de sleutel in de volgende situaties:

- Bij een stroomonderbreking
- Bij een opstartstoring
- Bij een storing in een onderdeel van de computer (zoals de processor of de voedingseenheid)
- Als u het wachtwoord bent vergeten

VOORZICHTIG: De Smart Cover FailSafe-sleutel is een speciaal hulpmiddel dat verkrijgbaar is bij HP. U kunt de sleutel het beste bestellen voordat u deze nodig heeft bij een HP Business of Service Partner.

Ga als volgt te werk om de FailSafe-sleutel te verkrijgen:

- Neem contact op met een HP Business Partner.
- Bel het telefoonnummer dat in de garantie wordt genoemd.

Raadpleeg voor meer informatie over het gebruik van de Smart Cover FailSafe-sleutel de *Naslaggids voor de hardware*.

Kabelslotvoorziening

De achterkant van de computer (bepaalde modellen) is voorzien van een kabelslot zodat de computer fysiek aan de werkplek kan worden bevestigd.

Raadpleeg voor geïllustreerde instructies de *Naslaggids voor de hardware*.

Vingerafdruktechnologie

Dankzij HP technologie voor de identificatie van vingerafdrukken is het niet langer nodig dat de eindgebruiker wachtwoorden invoert en wordt de netwerkbeveiliging verbeterd. Bovendien wordt het aanmelden vereenvoudigd en nemen de beheerkosten van bedrijfsnetwerken af. Aangezien deze optie gunstig geprijsd is, is deze niet uitsluitend voorbehouden aan hightech organisaties met behoefte aan strikte beveiliging.

OPMERKING: Ondersteuning van de technologie voor de identificatie van vingerafdrukken is afhankelijk van het model.

Foutmeldingen en herstel

Deze pc is uitgerust met voorzieningen voor foutberichten en foutherstel, waarbij innovatieve hard- en softwaretechnologie voorkomt dat essentiële gegevens verloren gaan en ongeplande uitvaltijd van de apparatuur tot een minimum beperkt blijft.

Als de computer is aangesloten op een netwerk dat wordt beheerd met HP Client Manager, worden de foutberichten naar de netwerkbeheerapplicatie gestuurd. Met HP Client Manager Software kunt u bovendien op alle beheerde computers op afstand geplande diagnoseprogramma's laten uitvoeren en een samenvatting laten weergeven van de niet-geslaagde tests.

Schijfbeveiligingssysteem

Het schijfbeveiligingssysteem DPS (Drive Protection System) is een diagnosehulpmiddel dat in de vaste schijf van bepaalde HP computers is ingebouwd. DPS is bedoeld om een diagnose te stellen van problemen met de vaste schijf, zodat de vaste schijf niet nodeloos wordt vervangen.

Tijdens de productie van HP bedrijfscomputers wordt elke geïnstalleerde vaste schijf met DPS getest en wordt de belangrijkste informatie permanent naar de schijf geschreven. Telkens wanneer DPS wordt uitgevoerd, worden de testresultaten naar de vaste schijf geschreven. De geautoriseerde Business of Service Partner gebruikt deze informatie om de omstandigheden te achterhalen die het uitvoeren van DPS noodzakelijk maakten. Raadpleeg de handleiding *Problemen oplossen* voor instructies over het gebruik van DPS.

Netvoeding met stroompiekbeveiliging

Een geïntegreerde voedingseenheid met stroompiekbeveiliging biedt grotere betrouwbaarheid bij onverwachte stroompieken. Hierdoor kan het systeem stroompieken van maar liefst 2.000 Volt weerstaan zonder dat het systeem uitvalt of dat er gegevens verloren gaan.

Warmtesensor

De temperatuursensor is een hardware- en softwarevoorziening waarmee de interne temperatuur van de computer wordt bewaakt. Deze voorziening geeft een waarschuwingsbericht weer wanneer het normale temperatuurbereik wordt overschreden, zodat u tijd heeft om actie te ondernemen voordat interne onderdelen worden beschadigd of gegevens verloren gaan.

△ **VOORZICHTIG:** Hoge systeemtemperaturen kunnen leiden tot schade aan het systeem of gegevensverlies.

Index