

# Handboken Hantera datorn

## Stationära datorer

© Copyright 2008 Hewlett-Packard Development Company, L.P. Informationen i detta dokument kan ändras utan föregående meddelande.

Microsoft, Windows och Windows Vista är antingen varumärken eller registrerade varumärken som tillhör Microsoft Corporation i USA och/eller andra länder.

Intel och vPro är varumärken som tillhör Intel Corporation i USA och andra länder.

Det enda garantiansvar för HP-produkter och HP-tjänster definieras i de uttryckliga garantiavtal som medföljer sådana produkter och tjänster. Ingenting i denna text skall anses utgöra ytterligare garantiåtaganden. HP ansvarar inte för tekniska fel, redigeringsfel eller för material som utelämnats i detta dokument.

Detta dokument innehåller information som omfattas av lagen om upphovsrätt. Ingen del av detta dokument får kopieras eller reproduceras i någon form utan skriftligt medgivande från Hewlett-Packard Company.

Hantering av bordsdatorer

Stationära datorer

Tredje upplagan (juli 2008)

Dokumentets artikelnummer: 451272-103

## Om den här boken

Denna handbok innehåller definitioner och instruktioner för säkerhetsfunktioner och hanterbarhet som finns förinstallerade i vissa modeller.

- △ **VARNING:** Den här texten ger information om att allvarliga personskador eller dödsfall kan uppstå om instruktionerna inte följs.
- △ **VIKTIGT:** Den här texten innehåller varningar om att utrustningen kan förstöras eller information förloras om inte instruktionerna följs.
- 📝 **OBS!** Text framhävd på det här sättet innehåller viktig extra information.



---

# Innehåll

## 1 Översikt hantering av bordsdatorer

## 2 Initial konfiguration och distribution

HP Software Agent .....	3
Altiris Deployment Solution Agent .....	3

## 3 Fjärrinstallation av system

## 4 Uppdatering och hantering av programvara

HP Client Management Interface .....	5
HP SoftPaq Download Manager .....	6
HP System Software Manager .....	7
HP ProtectTools Security Manager .....	7
HP Client Automation Starter och Standard Editions .....	8
HP Client Automation Enterprise Edition .....	8
HP Client Manager från Symantec .....	9
Altiris Client Management Suite .....	10
HP Client Catalog för Microsoft System Center- och SMS-produkter .....	10
HP Backup and Recovery Manager .....	11
Hanteringsteknik .....	12
Verdiem Surveyor .....	14
HP Proactive Change Notification (HP-meddelande om ändring av produkt) .....	14
Subscriber's Choice .....	14
Indragna lösningar .....	14

## 5 ROM-flash

Fjärruppgradering av flash-ROM .....	15
HPQFlash .....	15

## 6 Boot Block Emergency Recovery Mode

## 7 Replikera installation

Kopiera till en enstaka dator .....	17
-------------------------------------	----

Kopiera till flera datorer .....	18
Skapa en startbar enhet .....	19
USB-flashmedieenhet som stöds .....	19
USB-flashmedieenhet som inte stöds .....	20

## 8 Strömbrytare med två lägen

## 9 HP:S webbplats för Support

## 10 Industristandarder

## 11 Inventarietkontroll och säkerhet

Lösenordsskydd .....	28
Skapa ett setup-lösenord med setup-programmet .....	29
Skapa ett Start-lösenord med Setup-programmet .....	29
Ange ett startlösenord .....	29
Ange ett lösenord för Setup-programmet .....	30
Ändra ett start- eller setup-lösenord .....	30
Ta bort ett start- eller setup-lösenord .....	31
Avgränsare för nationellt tangentbord .....	31
Radera lösenord .....	31
DriveLock .....	32
Använda DriveLock .....	32
DriveLock-program .....	32
Smart Cover sensor .....	34
Ange skyddsnivå för SmartCover-sensor .....	34
Smart Cover Lock .....	34
Låsa med SmartCoverLock .....	35
Låsa upp SmartCoverLock .....	35
Använd FailSafe-nyckeln på Smart Cover-locket .....	35
Kabellåsfäste .....	36
Identifikation genom fingeravtryck .....	36
Felmeddelande och återställning .....	36
DPS (Drive Protection System) .....	36
Nättaggregat med överspänningsskydd .....	36
Termisk sensor .....	36

<b>Index .....</b>	<b>37</b>
--------------------	-----------

---


# 1 Översikt hantering av bordsdatorer

HP Client Management Solutions ger standardbaserade lösningar för hantering och kontroll av stationära och bärbara datorer samt arbetsstationer i nätverksmiljö. HP introducerade år 1995 branschens första system för fullständig styrbarhet av datorer. HP har patenterat tekniken för denna styrbarhet. Sedan dess har HP lett en branschgemensam strävan att ta fram nödvändig standard och infrastruktur för att effektivt kunna installera, konfigurera och styra stationära och bärbara datorer samt arbetsstationer. HP utvecklar egen styrprogramvara och samarbetar intimt med ledande tillverkare av styrprogramvara för att garantera en kompatibilitet mellan HP Client Management Solutions och deras produkter. HP Client Management Solutions är en viktig aspekt av ett omfattande åtagande att förse dig med lösningar som hjälper dig att sänka totalkostnaden för att äga och hantera datorerna genom hela deras livstid.

Huvudfunktionerna och fördelarna i datorhanteringen är:

- Initial konfiguration och installation
- Fjärrinstallation av dator
- Uppdatering och hantering av program
- ROM-uppdatering
- Konfigurering av maskinvarualternativ
- Inventarietkontroll och säkerhet
- Felmeddelanden och återställning

---

 **OBS!** Stödet för de olika funktionerna som beskrivs i handboken kan variera med modell och programversion.

---

---

## 2 Initial konfiguration och distribution

Datorn levereras med en förinstallerad systemprogramprofil. Efter en snabb "programuppackning" kan du börja använda datorn.

Du vill kanske byta ut den förinstallerade programprofilen mot en anpassad profil med system- och användarprogram. Det finns flera olika sätt att installera en egen programprofil. Dessa är:

- Installera extra program efter det att den förinstallerade programprofilen har packats upp.
- Använd programvarudistributionsverktyg, såsom HP Client Automation Standard Edition, HP Client Automation Enterprise Edition (baserat på Radia-teknik) eller Altiris Deployment Solution för att ersätta den förinlästa programvaran med en anpassad programvaruavbildning.
- Använda en diskkloningsprocess för att kopiera innehållet från en hårddisk till en annan.

Den bästa distributionsmetoden beror på din IT-miljö och processerna i den.

HP Backup and Recovery system, ROM-baserade installation och ACPI-maskinvara ger ytterligare hjälp vid återställning av systemprogramvara, konfigurationshantering och felsökning samt strömsparfunktioner.

---

 **OBS!** Se avsnittet [HP Backup and Recovery Manager på sidan 11](#) för mer information om hur du skapar en uppsättning återställningsskivor.

---



## HP Software Agent

Hanteringsagenten som används av både HP Client Automation Standard och Enterprise Edition är förinläst på datorn. När programmet har installerats är kommunikation möjlig med HP:s hanteringskonsol.

Så här installerar du HP Software Agent:

1. Klicka på **Start**.
2. Klicka på **Alla program**.
3. Klicka på **HP Manageability**.
4. Klicka på **Radia Management Agent Readme**.
5. Granska och följ instruktionerna i Readme-filen för att installera HP Software Agent.

HP Software Agent är en nyckelkomponent i infrastrukturen som används för att aktivera alla HP Client Automation-lösningar. Mer information om andra infrastrukturkomponenter som behövs vid implementering av HP-lösningar för konfigurationshantering finns på <http://h20229.www2.hp.com/solutions/ascm/index.html>.

## Altiris Deployment Solution Agent

Detta program är förinläst på datorn. När programmet har installerats är kommunikation möjlig med administratörskonsolen Deployment Solution.

Så här installerar du Altiris Deployment Solution Agent:

1. Klicka på **Start**.
2. Klicka på **Alla program**.
3. För Windows Vista klickar du på **Installera Altiris DAgent**. För Windows XP klickar du på **Installera Altiris AClient**.
4. Följ instruktionerna på skärmen för att installera och konfigurera Altiris-klienten.

Den här agenten är en nyckelkomponent i infrastrukturen för att aktivera Altiris Deployment Solution, som är en del av Altiris Client Management Suite. Mer information om andra infrastrukturkomponenter som behövs vid implementering av Altiris Client Management Suite finns på <http://www.hp.com/go/easydeploy>.

---

## 3 Fjärrinstallation av system

Med Remote System Installation kan du starta och konfigurera systemet genom att använda programvaru- och konfigurationsinformationen som finns på en nätverksserver genom att initiera PXE (Preboot Execution Environment). Remote System Installation-funktionen används normalt som ett verktyg för systeminstallation och systemkonfiguration och kan användas till följande uppgifter:

- Formatera en hårddisk
- Installera en programprofil i en eller flera nya persondatorer
- Fjärruppdatering av systemets BIOS i flash-ROM ([Fjärruppdatering av flash-ROM på sidan 15](#))
- Konfigurera systemets BIOS-inställningar

För att starta fjärrinstallation trycker du på **F12** när meddelandet **F12 = Network Service Boot** visas i nedre högra hörnet på bilden med HP:s logotyp medan datorn startar. Följ instruktionerna på skärmbilden och fortsätt proceduren. Standardstartordningen är en BIOS-konfigurationsinställning som kan ändras så att den alltid försöker starta från PXE.

---

## 4 Uppdatering och hantering av programvara

HP tillhandahåller flera verktyg för hantering och uppdatering av programvara i stationära datorer, arbetsstationer och bärbara datorer:

- HP Client Management Interface
- HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools Security Manager
- HP Client Automation Starter, både Standard och Enterprise Edition
- HP Client Manager från Symantec
- Altiris Client Management Suite
- HP Client Catalog för Microsoft System Center- och SMS-produkter
- HP Backup and Recovery Manager
- Intel vPro-märkta datorer med Active Management Technology
- Verdiem Surveyor
- HP Proactive Change Notification (HP-meddelande om ändring av produkt)
- HP Subscriber's Choice

### HP Client Management Interface

Det är viktigt att hantera både maskinvaru- och programvaruresurser väl för att hålla IT-kostnaderna nere och affärsverksamheten flexibel. Detta gäller oavsett vilka systemhanteringsverktyg din IT-avdelning använder. IT-administratören kan komma åt HP Client Management-gränssnittet genom att skriva enkla skript och integrera de skripten i de hanteringslösningar de passar för.

Med HP Client Management Interface (HP CMI), integreras HP:s nya affärsdatorer smidigt i hanteringen av din IT-miljö. HP CMI tillhandahåller ett gränssnitt som förenklar integreringen av HP:s affärsdatorer med populära hanteringsverktyg för industrisystem (inklusive Microsoft Systems Management Server, IBM Tivoli Software och HP Operations) och anpassade, internt utvecklade hanteringsprogram. Med hjälp av HP CMI kan systemhanteringsverktyg och program få djuplodande tillgång till klientresurser, få hälsostatusinformation och hantera BIOS-inställningar för system genom att direkt kommunicera med

klientdatorn, vilket minskar behovet av agenter eller anslutningsprogramvara för att uppnå full integrering.

HP Client Management Interface baseras på industristandarder som inkluderar Microsoft Windows Management Interface (MS WMI), Web-Based Enterprise Management (WBEM), System Management BIOS (SMBIOS) och Advanced Configuration and Power Interface (ACPI). HP CMI är en grundläggande teknologi som användes i HP Client Management Solutions. Med HP CMI ger HP dig flexibilitet när du väljer hur du ska hantera dina HP-klientdatorer.

HP Client Management Interface använt tillsammans med systemhanteringsprogramvara kan

- skaffa ingående klientresursinformation — ger detaljerad information om processorerna, hårddiskar, minne, BIOS, drivrutiner inklusive sensorinformation (såsom fläkthastighet, spänning och temperatur)
- ta emot hälsostatusinformation — abonnerar på en rad maskinvarumeddelanden från klienten (såsom temperaturgränsöverskridanden, fläktstopp och konfigurationsändringar i hårdvaran) som sedan sänds till systemhanteringskonsollen, program eller den lokala klientdatorn. Varningar skickas i realtid när de skapas av maskinvaruhändelser.
- hantera system BIOS-inställningar — utför F10-funktioner inklusive inställning och ändring av BIOS-lösenord och datorns startordning, allt från systemhanteringskonsollen på vilket som helst av dina klientsystem. Du behöver inte gå till varje enskild dator.

Mer information om HP Client Management Interface finns på <http://www.hp.com/go/hpcmi/>.

## HP SoftPaq Download Manager


HP SoftPaq Download Manager är ett gratis lättanvänt gränssnitt som gör att du kan både hitta och hämta programvaruuppdateringar för HP-klientdatorerna i din miljö. Genom att ange dina modeller, operativsystem och språk kan du snabbt hitta, sortera och markera de programvarupaket (softpaqs) du behöver. Du kan hämta HP SoftPaq Download Manager från <http://www.hp.com/go/sdm>.

# HP System Software Manager

HP System Software Manager (SSM) är ett kostnadsfritt program som automatiserar fjärrspridning av drivrutins- och BIOS-uppdateringar för ditt nätverks stationära arbetsdatorer från HP. När SSM körs, fastställer det automatiskt (utan användarens medverkan) versionsnivåerna hos drivrutiner och BIOS som installerats i alla datorerna i nätverket och jämför dessa data med systemets programvaru-SoftPaqs, som har testats och lagrats i ett centralt filarkiv. SSM uppdaterar därefter automatiskt alla gamla versioner av nätverkssystemets programvara till de senaste versionerna som finns i filarkivet. Eftersom SSM endast tillåter distribution av SoftPaq-uppdateringar till rätt klientsystemmodeller, kan administratören förtroendefullt och effektivt använda SSM för att hålla systemets programvara uppdaterad.

System Software Manager integreras med distributionsverktyg för företagsprogram, såsom HP Client Automation solutions, HP Client Manager från Symantec och Microsoft Systems Management Server (SMS). Med hjälp av SSM kan du distribuera kund- eller tredjepartsuppdateringar som har förpackats i SSM-formatet.

SSM kan hämtas kostnadsfritt från <http://www.hp.com/go/ssm>.

 **OBS!** SSM stöder för närvarande inte fjärruppggradering av flash-ROM på system som har aktiverat Windows Vista BitLocker och som använder TPM-mätningar för att skydda BitLocker-nycklarna eftersom uppggradering av BIOS skulle göra att den signatur som BitLocker skapade för plattformen blev ogiltig. Inaktivera BitLocker via grupp-principen om du vill uppdatera systemets BIOS.

Du kan aktivera BitLocker-stöd utan TPM-mätningar av BIOS för att undvika att BitLocker-nycklar ogiltigförklaras. HP rekommenderar att du behåller en säkerhetskopia av BitLocker-uppgifterna i händelse av nödfall.

# HP ProtectTools Security Manager

Programvaran HP ProtectTools Security Manager innehåller säkerhetsfunktioner som ger skydd mot obehörig åtkomst av datorn, nätverk och kritiska data. Följande programvarumoduler tillhandahåller utökade säkerhetsfunktioner:

- Credential Manager for HP ProtectTools
- Embedded Security for HP ProtectTools
- Java Card Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Device Access Manager for HP ProtectTools
- File Sanitizer för HP ProtectTools
- Privacy Manager för HP ProtectTools

Beroende på vilken datormodell du har, kan de tillgängliga programvarumodulerna variera. Embedded Security for HP ProtectTools är t ex bara tillgängligt på datorer där det inbäddade säkerhetschipet för "trusted platform module" (TPM) är installerat.

HP ProtectTools-programvarumoduler kan vara förinstallerade, förinladdade eller möjliga att ladda ned från HP:s webbplats. För utvalda HP Compaq-skrivbordsdatorer är HP ProtectTools tillgängligt som ett eftermarknadstillval. Mer information finns på <http://www.hp.com/products/security>.

## HP Client Automation Starter och Standard Editions

HP Client Automation är en lösning för hantering av maskin- och programvara för miljöerna Windows Vista, Windows XP och HP Thin Client. Den är enkel att använda och kan distribueras snabbt samtidigt som den är en stabil grund för framtida behov. Den finns i två versioner:

- Starter Edition är en gratisprodukt för hantering av stationära och bärbara HP-datorer samt arbetsstationer. Den erbjuder maskinvaru- och programvaruinventering, fjärrstyrning, HP-övervakning av varningar, uppdatering av HP BIOS och drivrutiner, integrering med HP Protect Tools och tilläggsupport för Intel AMT. Starter Edition stöder också distribution och hantering av HP Thin Clients.
- Standard Edition, som kan köpas, innehåller förutom alla funktioner från Starter Edition, distribution och migrering av Windows, möjlighet till patch-hantering, programvarudistribution samt mätning av programanvändning.

HP Client Automation Starter Edition och Standard Edition erbjuder en migreringssökväg till HP Client Automation Enterprise Edition (baserad på Radia-teknik) för automatiserad hantering av stora, heterogena och ständigt föränderliga IT-miljöer.

Mer information om HP Client Automation solutions finns på <http://www.hp.com/go/client>.

## HP Client Automation Enterprise Edition

HP Client Automation Enterprise Edition är en policybaserad lösning med vilken administratörer kan inventera, sprida, uppdatera och fortlöpande hantera programvara och innehåll över heterogena klientplattformar. Med hjälp av HP Client Automation Enterprise Edition, kan IT-administratörer:

- Automatisera hanteringsprocessen för hela livscykeln från upptäckt, spridning och pågående hantering genom migrering och retirement (avställning)
- Distribuera och hantera kontinuerligt och automatiskt alla program (operativsystem, program, patchar, inställningar och innehåll) till önskat tillstånd
- Hantera programvara på alla enheter, inklusive stationära och bärbara datorer, i en homogen eller fristående infrastruktur
- Hantera programvara på de flesta operativsystem

Med kontinuerlig konfigurationshantering rapporterar HP-kunder dramatiska besparingar av IT-kostnader, kortare tid tills program och innehåll når marknaden samt ökad användarproduktivitet och tillfredsställelse.

Mer information om HP Client Automation-lösningar finns på <http://www.hp.com/go/client>.

## HP Client Manager från Symantec

HP Client Manager från Symantec, utvecklad med Altiris, finns tillgänglig utan kostnad för alla bärbara och stationära HP-datorer och arbetsstationer som stöds. SSM är integrerad i HP Client Manager och möjliggör central spårning, övervakning samt hantering av maskinvaruaspekter i HP-klientsystem.

HP Client Manager från Symantec hjälper dig att:

- Erhålla värdefull maskinvaruinformation såsom CPU-, minnes-, bild- och säkerhetsinställningar
- Övervaka systemets "hälsa" för att åtgärda problem innan de uppstår
- Erhålla och automatiskt installera drivrutiner och BIOS-uppdateringar utan att gå till varje enskild dator
- Fjärrkonfigurera BIOS- och säkerhetsinställningar
- Automatisera processer för att snabbt åtgärda maskinvaruproblem

En nära integration med verktygen i HP Instant Support minskar tiden för felsökning av maskinvara.

- Diagnostik — fjärrkör visningsrapporter om HP:s stationära, bärbara och arbetsstationdatormodeller
- Systemhälsoskanning — letar efter kända maskinvaruproblem i din installerade bas med HP klientsystem
- Aktiv chatt — anslut till HP:s kundtjänst för att söka svar på problem
- HP Knowledgebase — länk till expertinformation
- Automatisk SoftPaq-kollektion och leveransprocess för snabba lösningar på maskinvaruproblem
- Identifiera, inventera och initialisera system med HP ProtectTools inbäddade säkerhetschip
- Alternativ för hälsomeddelanden som visas lokalt på klientsystemet
- Rapportera basresursinformation om icke HP-klienter
- Installera och konfigurera TPM-säkerhetschipet
- Central schemaläggning av klientsäkerhetskopiering och -återställning
- Ytterligare stöd för att hantera Intel AMT

Mer information om HP Client Manager från Symantec finns på <http://www.hp.com/go/clientmanager>.

## Altiris Client Management Suite

Altiris Client Management Suite är en lättanvänd lösning för att administrera programvara för arbetsstationer, stationära och bärbara datorer under hela deras livscykel. Client Management Suite Level 1 innehåller följande Altiris-produkter:

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

Mer information om Altiris Client Management Suite finns på <http://www.altiris.com/Products/ClientManagementSuite.aspx>.

## HP Client Catalog för Microsoft System Center- och SMS-produkter

HP Client Catalog gör det möjligt för IT-administratörer att använda Microsoft-produkter för att automatisera distributionen av HP:s programvaruuppdateringar (Softpaqs) till HP-datorer i företaget. Katalogfilen innehåller detaljerad plattformsinformation för skrivbordsdatorer samt bärbara datorer och arbetsstationer i företaget. Det kan användas i förening med de anpassade inventerings- och uppdateringsfunktioner för Microsoft-produkter som ger automatiserade drivrutin- och patchuppdateringar för hanterade HP-klientdatorer.

Microsoft-produkter som stöds av HP Client Catalog inkluderar:

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

Mer information om HP Client Catalog för SMS finns på <http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html>.



# HP Backup and Recovery Manager

HP Backup and Recovery Manager är ett lättanvänt, mångsidigt program som gör det möjligt för dig att säkerhetskopiera och återställa hårddisken på datorn. Programmet fungerar i Windows för att göra säkerhetskopior av Windows, alla program och alla datafiler. Säkerhetskopieringar kan schemaläggas så att de automatiskt sker vid angivna intervall, eller också kan de startas manuellt. Viktiga filer kan arkiveras separat från normala säkerhetskopior.

HP Backup and Recovery Manager är förinstallerat på C-enheten och skapar en återställningspartition.


Återställningspunkter och säkerhetskopior kan kopieras till CD- eller DVD-skivor medan alla säkerhetskopior kan kopieras till nätverket eller sekundära hårddiskar.

HP rekommenderar starkt att du skapar en uppsättning återställningsskivor direkt innan du börjar använda datorn och att du schemalägger regelbundna, automatiska säkerhetskopieringar med återställningspunkter.

Skapa en uppsättning återställningsskivor:

1. Klicka på **Start > HP Backup and Recovery > HP Backup and Recovery Manager** för att öppna guiden till Backup and Recovery. Klicka sedan på **Nästa**.
2. Klicka på **Skapa återställningsskivor (rekommenderas)** och klicka på **Nästa**.
3. Följ instruktionerna i guiden.

Mer information om hur du använder HP Backup and Recovery Manager finns i *Användarhandboken HP Backup and Recovery Manager* som du hittar genom att välja **Start > HP Backup and Recovery > HP Backup and Recovery Manager Manual**.

 **OBS!** Du kan beställa återställningsskivor från HP genom att ringa till HP support center. Gå till följande webbplats, välj region och klicka på länken **Technical support after you buy** (Teknisk support efter köp) under rubriken **Call HP** (Ring HP) om du vill få telefonnumret till supportcentret i din region.

[http://welcome.hp.com/country/us/en/wwcontact\\_us.html](http://welcome.hp.com/country/us/en/wwcontact_us.html)


# Hanteringsteknik

Modeller inkluderar antingen vPro-teknik eller standardteknik. Båda medger bättre upptäckt, avhjälpning och skydd av datorer i nätverket. Båda tekniker gör att datorer kan hanteras oavsett om systemet är påslaget, avstängt eller om operativsystemet har hängit sig.

Funktioner för hanteringsteknik inkluderar:

- inventeringsinformation om maskinvara
- varningsmeddelanden
- strömsparfunktioner — ström på/av, återanvänd ström
- fjärrdiagnostik och -reparation
  - Serial-over-LAN — tillåter konsolstyrning av en fjärrdator under startfasen.
  - IDE-Redirect — tillåter systemstart från en fjärrstartenhet, skiva eller ISO-avbildning
- maskinvarubaserad isolering och återställning — begränsar eller stänger helt av åtkomst till en dator om misstänkt virusaktivitet upptäcks

---

 **OBS!** En översikt av Intel vPro-tekniken finns på <http://www.intel.com/vpro>.

Se faktabladerna på <http://www.hp.com/support> om du vill läsa HP-specifik information om Intel vPro-tekniken. Välj ditt land och språk, välj **Se information om support och felsökning**, ange datorns modellnummer och tryck på **Retur**. Klicka på **Manualer (handböcker, supplement, tillägg etc)** i kategorin **Resurser**. Klicka på **White papers** under **Genväg till manualer via kategori**.

---

Tillgängliga hanteringstekniker inkluderar följande:


- AMT (inkluderar DASH 1.0)
- ASF

Både ASF och AMT stöds, men de kan inte konfigureras samtidigt.

Så här konfigurerar du Intel vPro-system för AMT eller ASF:

1. Starta eller starta om datorn. Om du är i Microsoft Windows klickar du på **Start > Stäng av > Starta om datorn**.
2. Så snart datorn har startat, tryck på snabbtangenter **Ctrl+P**, innan operativsystemet startar på datorn.

---

 **OBS!** Om du inte trycker på **Ctrl+P** vid rätt tillfälle, måste du stänga av datorn, starta om den och trycka på **Ctrl+P** innan operativsystemet startar på datorn för att komma åt programmet.

---

Denna snabbvalssekvens startar verktyget Intel Management Engine BIOS Execution (MEBx). Detta verktyg hjälper användaren att konfigurera olika aspekter av hanteringstekniken. Några av konfigurationsalternativen är listade nedan:

- Huvudmeny
  - Intel ® ME-konfigurering
  - Intel ® AMT-konfigurering
  - Ändra Intel ® ME-lösenord
  - Avsluta
- Intel ® ME Platform-konfigurering
  - Intel ® ME State Control (aktivera/inaktivera)
  - Intel ® ME Firmware Local Update (aktivera/inaktivera)
  - Intel ® ME Features Control
  - Intel ® ME Power Control
- Intel ® AMT-konfigurering
  - Värddatornamn
  - TCP/IP
  - Provision Model (Enterprise, SMB)
  - Installation och konfiguration
  - Stänga av
  - SOL/IDE-R (aktivera/inaktivera)
  - Lösenordspolicy
  - Secure Firmware Update (aktivera/inaktivera)
  - Konfigurera PRTC
  - Timeout för viloläge
- Ändra Intel ® ME-lösenord (HP rekommenderar starkt att det här lösenordet ändras. Standardlösenordet är **admin**.)

Om administratören vill fjärrhantera AMT-system måste han/hon använda en fjärrkonsol som stöder AMT. Konsoler för företagshantering finns hos leverantörer såsom HP, Altiris och Microsoft SMS. I SMB-läge tillhandahåller klienten ett webbläsargränssnitt. Du kommer åt denna funktion genom att öppna en läsare från valfritt system på nätverket och ange `http://värd_namn:16992` där `värd_namn` är systemets namn. Alternativt kan IP-adressen användas istället för värdnamnet.

## Verdiem Surveyor

Verdiem Surveyor är en programvarulösning som hjälper till att hantera datorernas energiförbrukning. Surveyor mäter och rapporterar hur mycket energi varje dator förbrukar. Programmet ger även kontroll över datorernas energisparinställningar så att administratörer enkelt kan införa besparingsstrategier i hela nätverket. Ett HP SoftPak med Surveyor-agenten kan hämtas från HP:s supportwebbplats och kan installeras på de kommersiella stationära datormodeller som stöds. Du kan köpa Surveyor-licenser för datoradministration från din HP-representant.

## HP Proactive Change Notification (HP-meddelande om ändring av produkt)

PCN-programmet använder Subscriber's Choice-webbplatsen för att proaktivt och automatiskt:

- Skicka PCN-meddelanden (Product Change Notification) till dig via e-post för att informera dig om ändringar av maskin- och programvara för flertalet kommersiella datorer och servrar, upp till 60 dagar i förväg.
- Skicka e-post med Kund-, Råd-, Upplysnings- och Säkerhetsmeddelanden samt drivrutinvarningar till dig för flertalet kommersiella datorer och servrar.

Du skapar din egen profil, så att du bara erhåller den typ av information som är viktig för en viss IT-miljö. Mer information om Proactive Change Notification-programmet och om hur du skapar en anpassad profil finns på adressen <http://h30046.www3.hp.com/subhub.php>.

## Subscriber's Choice

Subscriber's Choice är ett klientbaserat program från HP.

Baserat på din profil, tillhandahåller HP personliga produkttips, artiklar och/eller varningar/meddelanden om drivrutiner och support.

Subscriber's Choice Driver och Support Alerts/Notifications skickar e-postmeddelanden om att den information som du valde att prenumerera på i din profil finns tillgänglig för granskning och hämtning. Läs mer om Subscriber's Choice och hur du skapar en anpassad profil på <http://h30046.www3.hp.com/subhub.php>.

## Indragna lösningar

Två programvaror, Altiris Local Recovery och Dantz Retrospect, kommer inte längre att levereras med HP:s stationära datorer, notebooks eller arbetsstationer. Nya stationära datorer, notebooks eller arbetsstationer som släpps under 2006 kommer att levereras med HP Backup and Recovery Manager.

---

## 5 ROM-flash

Datorns BIOS är lagrat i ett programmerbart flash-ROM (read only memory = skrivskyddat minne). Genom att ställa in ett setup-lösenord i setup-programmet (F10) kan du skydda ROM från att oavsiktligt uppdateras eller skrivs över. Det är viktigt för att garantera datorns driftsäkerhet. Om du skulle behöva uppgradera BIOS, kan du ladda ned de senaste BIOS-avbildningarna från HP:s drivrutins- och supportsida, <http://www.hp.com/support/files>.

- △ **VIKTIGT:** För att få ett maximalt ROM-skydd ställer du in ett lösenord för Setup-programmet. Lösenordet skyddar mot obehörig ROM-uppgradering. Med SSM (System Software Manager) kan systemadministratören ställa in setup-lösenord på en eller flera datorer samtidigt. Mer information finns på <http://www.hp.com/go/ssm>.

### Fjärruppgradering av flash-ROM

Med hjälp av fjärruppgradering av ROM kan systemadministratören göra en säker BIOS-fjärruppgradering på HP-datorer direkt från en central plats i nätverket. Systemadministratören kan uppgradera flera datorer centralt vilket ger en mer konsistent utveckling och större kontroll över HP PC BIOS-avbildningar över nätverket. Det ger också högre produktivitet och lägre total ägandekostnad.

- 📌 **OBS!** SSM stöder för närvarande inte fjärruppgradering av flash-ROM på system som har aktiverat Windows Vista BitLocker och som använder TPM-mätningar för att skydda BitLocker-nycklarna eftersom uppgradering av BIOS skulle göra att den signatur som BitLocker skapade för plattformen blev ogiltig. Inaktivera BitLocker via grupp-principen om du vill uppgradera systemets BIOS.

Datorn måste vara på eller startas med Remote Wakeup ("fjärrväckning") för att du ska kunna dra fördel av fjärruppgraderingen av ROM.

Mer information om Fjärruppgradering av Flash-ROM finns under HP Client Manager Software eller System Software Manager på <http://www.hp.com/go/ssm/>.

### HPQFlash

Verktyget HPQFlash används för att lokalt uppdatera eller återställa system-BIOS på enskilda datorer från ett Windows-operativsystem.

Mer information om HPQFlash finns på <http://www.hp.com/support/files>. Ange datorns modellnummer när du uppmanas till det.

## 6 Boot Block Emergency Recovery Mode

Ett startblock i katastrofåterställningsläge gör att systemet kan återställas vid den osannolika händelsen att en ROM-uppgradering misslyckas. Om t ex ett strömavbrott inträffar under en BIOS-uppgradering, blir ROM-uppgraderingen inkomplett. Detta kommer att göra system-BIOS oanvändbart. Startblocket är en flash-skyddad sektion av ROM som innehåller kod som kontrollerar att en giltig system BIOS-avbildning finns varje gång systemet startas.

- Om system BIOS-avbildningen är giltig startar systemet normalt.
- Om systemets BIOS-avbildning är felaktig, kommer ett felsäkert startblocks-BIOS att ge tillräckligt stöd för att söka efter löstagbara media för BIOS-avbildningsfiler. Om en giltig BIOS-avbildningsfil hittas, uppgraderas ROM automatiskt med den.

Om en ogiltig system BIOS-avbildning upptäcks, blinkar strömlampan rött 8 gånger med en sekunds mellanrum. Samtidigt piper högtalaren 8 gånger. Om partitionen med system-ROM som innehåller visningsalternativet ROM-avbildning inte är korrupt, visas **Boot Block Emergency Recovery Mode** på skärmen.

För att återställa systemet från detta läge gör du på följande sätt:

1. Stäng av strömmen.
2. Sätt in en cd eller USB-uppgraderingsenhet som innehåller den önskade BIOS-avbildningsfilen i rotkatalogen.



**OBS!** Mediet måste formateras med hjälp av filsystemen FAT12, FAT16 eller FAT32.

3. Starta datorn.

Om ingen lämplig BIOS-avbildning hittas, kommer du att uppmanas att sätta in media som innehåller en BIOS-avbildningsfil.

Om systemet lyckas omprogrammera ROM, kommer det sedan automatiskt att stängas av.

4. Ta bort det flyttbara media som användes för att uppgradera BIOS.
5. Sätt på strömmen igen för att starta om datorn.



**OBS!** BitLocker hindrar Windows Vista från att starta när en cd som innehåller BIOS-avbildningsfil finns i en optisk enhet. Om BitLocker aktiveras ska du ta bort den här cd:n innan du försöker starta med Windows Vista.

# 7 Replikera installation


Med de följande procedureerna kan administratören enkelt kopiera en installationskonfiguration till andra datorer av samma modell. Det ger en snabbare, mer konsistent konfiguration av flera datorer.

 **OBS!** Båda procedurer kräver en diskettenhet eller en USB-flashenhet som stöds.

## Kopiera till en enstaka dator

△ **VIKTIGT:** En installationskonfiguration är modellspecifik. Filsystemfel kan uppstå om käll- och måldatorer inte är av samma modell. Kopiera t ex inte en installationskonfiguration från en dc7xxx-PC till en dx7xxx-PC.

1. Välj installationskonfiguration att kopiera. Stäng av datorn. Om du är i Windows klickar du på **Start > Stäng av > Stäng av**.
2. Om du använder en USB flashmediaenhet, sätter du in den nu.
3. Starta datorn.
4. Så snart datorn har startat, tryck på snabbtangentsen **F10** innan operativsystemet startar på datorn för att komma åt Setup-programmet. Om du vill kan du trycka på **Retur** för att komma förbi titelskärmen.

 **OBS!** Om du inte trycker på **F10** vid rätt tillfälle, måste du stänga av datorn, starta om den och trycka på **F10** innan operativsystemet startar på datorn för att komma åt programmet.

5. Om du använder en diskett, sätter du in den nu.
6. Klicka på **Arkiv > Replikerad setup > Spara till flyttbart media**. Följ instruktionerna på skärmen för att skapa konfigurationsdisketten eller USB-flashmediaenheten.
7. Stäng av datorn som ska konfigureras och sätt in konfigurationsdisketten eller USB-flashmediaenheten.
8. Starta om datorn som ska konfigureras.
9. Så snart datorn har startat, tryck på snabbtangentsen **F10** innan operativsystemet startar på datorn för att komma åt Setup-programmet. Om du vill kan du trycka på **Retur** för att komma förbi titelskärmen.
10. Klicka på **Arkiv > Replikerad setup > Återställ från flyttbart media** och följ instruktionerna på skärmen.
11. Starta om datorn när konfigurationen är klar.

## Kopiera till flera datorer

- △ **VIKTIGT:** En installationskonfiguration är modellspecifik. Filsystemfel kan uppstå om käll- och måldatorer inte är av samma modell. Kopiera t ex inte en installationskonfiguration från en dc7xxx-PC till en dx7xxx-PC.

Den här metoden kräver lite mer tid för preparation av konfigurationsdisketten eller USB-flashmediaenheten, men det går väsentligt mycket fortare att kopiera konfigurationen till måldatorerna.

- 📝 **OBS!** För den här proceduren krävs en startbar diskett eller USB-flashmediaenhet. Om Windows XP inte är tillgängligt för att skapa en startbar diskett, kan du använda metoden för att kopiera till en enskild dator istället (se [Kopiera till en enskild dator på sidan 17](#)).

1. Skapa en startbar diskett eller USB-flashmediaenhet. Se [USB-flashmediaenhet som stöds på sidan 19](#) eller [USB-flashmediaenhet som inte stöds på sidan 20](#).

- △ **VIKTIGT:** Alla datorer kan inte startas från en USB-flashmediaenhet. Om den standardmässiga startordningen i setup-programmet (F10) anger USB-enheten före hårddisken, kan datorn startas från en USB-flashmediaenhet. I annat fall måste en startdiskett användas.

2. Välj installationskonfiguration att kopiera. Stäng av datorn. Om du är i Windows klickar du på **Start > Stäng av > Stäng av**.
3. Om du använder en USB-flashmediaenhet, sätter du in den nu.
4. Starta datorn.
5. Så snart datorn har startat, tryck på snabbtangenter **F10** innan operativsystemet startar på datorn för att komma åt Setup-programmet. Om du vill kan du trycka på **Retur** för att komma förbi titelskärmen.

- 📝 **OBS!** Om du inte trycker på **F10** vid rätt tillfälle, måste du stänga av datorn, starta om den och trycka på **F10** innan operativsystemet startar på datorn för att komma åt programmet.

6. Om du använder en diskett, sätter du in den nu.
7. Klicka på **Arkiv > Replikerad setup > Spara till flyttbart media**. Följ instruktionerna på skärmen för att skapa konfigurationsdisketten eller USB-flashmediaenheten.
8. Hämta ett BIOS-verktyg för att replikera installationen (repset.exe) och kopiera den till konfigurationsdisketten eller USB-flashmediaenheten. Detta verktyg får du genom att gå till <http://welcome.hp.com/country/us/en/support.html> och ange datorns modellnummer.
9. Skapa en autoexec.bat-fil innehållande följande kommando på konfigurationsdisketten eller USB-flashmediaenheten.

```
repset.exe
```

10. Stäng av datorn som ska konfigureras. Sätt in konfigurationsdisketten eller USB-flashmediaenheten och sätt på datorn. Konfigurationsverktyget körs automatiskt.
11. Starta om datorn när konfigurationen är klar.



# Skapa en startbar enhet

## USB-flashmediaenhet som stöds

Enheter som stöds har en förinstallerad avbildning för att förenkla processen att göra dem startbara. Alla HP- eller Compaq- och de flesta andra USB flashmediaenheter har denna förinstallerade avbildning. Om den USB-flashmediaenhet som används saknar avbildningen, använder du proceduren senare i det här avsnittet (se [USB-flashmediaenhet som inte stöds på sidan 20](#)).

För att skapa en startbar USB-flashmediaenhet måste du ha:

- en stödd USB-flashmediaenhet
- en startbar DOS-diskett med programmen FDISK och SYS. (Om inte SYS är tillgängligt kan FORMAT användas, men alla befintliga filer på USB-flashmediaenheten förloras.)
- en PC som är startbar från en USB-flashmediaenhet

△ **VIKTIGT:** Vissa äldre PC:s är inte startbara från en USB-flashmediaenhet. Om den standardmässiga startordningen i setup-programmet (F10) anger USB-enheten före hårddisken, kan datorn startas från en USB-flashmediaenhet. I annat fall måste en startdiskett användas.

1. Stäng av datorn.
2. Sätt USB-flashmediaenheten i en av datorns USB-portar och ta bort alla övriga USB-lagringsenheter utom USB-diskettenheterna.
3. Sätt i en startbar DOS-diskett med FDISK.COM och antingen SYS.COM eller FORMAT.COM i en diskettenhet och sätt på datorn så att den startar upp från DOS-disketten.
4. Kör FDISK från **A:\** i kommandotolken genom att skriva `FDISK` och trycka på **Retur**. Vid uppmaning klickar du på **Ja (J)** för att aktivera stöd för stora disketter.
5. Ange Choice (Urval) [5] för att visa enheterna i systemet. Drive Key blir den enhet som storleksmässigt passar bäst bland enheterna i listan. Oftast är det den sista enheten i listan. Anteckna enhetsbokstaven.

USB-flashmediaenhet \_\_\_\_\_

△ **VIKTIGT:** Fortsätt inte om en enhet inte passar USB-flashmediaenheten. Dataförluster kan uppstå. Kontrollera om det finns ytterligare lagringsenheter i någon av USB-portarna. Om det finns någon tar du bort den, startar om datorn och fortsätter från steg 4. Om det inte finns någon stöder antingen systemet inte USB-flashmediaenheten eller så är USB-flashmediaenheten trasig. Fortsätt **INTE** att försöka göra USB-flashmediaenheten startbar.

6. Avsluta FDISK genom att trycka på **Esc** för att gå tillbaka till **A:\**-prompten.
7. Gå till steg 8 om den startbara DOS-disketten innehåller SYS.COM. Gå i annat fall till steg 9.
8. Vid **A:\**-prompten skriver du `SYS x:` där x representerar enhetsbokstaven ovan.

△ **VIKTIGT:** Kontrollera att du har skrivit korrekt enhetsbokstav för USB-flashmediaenheten.

När systemfilerna har överförts återgår SYS till **A:\**-prompten. Gå till steg 13.

9. Kopiera alla filer som du vill bevara från USB-flashmediaenheten i en temporär mapp i en annan enhet (till exempel systemets hårddisk).

10. Vid **A:\** skriver du `FORMAT /S X:` där X representerar enhetsbokstaven som nämndes ovan.


△ **VIKTIGT:** Kontrollera att du har skrivit korrekt enhetsbokstav för USB-flashmediaenheten.

FORMAT kommer att visa ett eller flera meddelanden och fråga dig varje gång om du vill fortsätta. Ange **J** varje gång. FORMAT kommer att formatera USB-flashmediaenheten, lägga till systemfilerna och fråga efter en volymetikett

11. Tryck på **Retur** om du inte vill ange etikett eller ange, om du så önskar, en etikett.

12. Kopiera tillbaka eventuella filer som du sparade i steg 9 till USB-flashmediaenheten.

13. Ta ur disketten och starta om datorn. Datorn startar nu upp från USB-flashmediaenheten som enhet C.

 **OBS!** Den standardmässiga startordningen varierar från dator till dator och kan ändras i setup-programmet (F10).

Om du har använt en DOS-version från Windows 9x, visas Windows-logon en kort stund. Om du inte vill att den här bilden ska visas, lägger du till en fil med längden noll och namnet LOGO.SYS i rotkatalogen på USB-flashmediaenheten.

Gå tillbaka till [Kopiera till flera datorer på sidan 18](#).

## USB-flashmediaenhet som inte stöds

För att skapa en startbar USB-flashmediaenhet måste du ha:

- en USB-flashmediaenhet
- en startbar DOS-diskett med programmen FDISK och SYS. (Om inte SYS är tillgängligt kan FORMAT användas, men alla befintliga filer på USB-flashmediaenheten förloras.)
- en PC som är startbar från en USB-flashmediaenhet

△ **VIKTIGT:** Vissa äldre PC:s är inte startbara från en USB-flashmediaenhet. Om den standardmässiga startordningen i setup-programmet (F10) anger USB-enheten före hårddisken, kan datorn startas från en USB-flashmediaenhet. I annat fall måste en startdiskett användas.

1. Om det finns något PCI-kort i systemet med anslutna SCSI-, ATA RAID- eller SATA-enheter, stänger du av datorn och drar ur nätsladden.


△ **VIKTIGT:** Nätsladden får INTE vara ansluten.

2. Öppna datorn och ta bort PCI-korten.

3. Sätt USB-flashmediaenheten i en av datorns USB-portar och ta bort alla övriga USB-lagringseinheter utom USB-diskettenheterna. Sätt tillbaka datorns lock.

4. Sätt i nätsladden och starta datorn.


5. Så snart datorn har startat, tryck på snabbtangenter **F10** innan operativsystemet startar på datorn för att komma åt Setup-programmet. Om du vill kan du trycka på **Retur** för att komma förbi titelskärmen.

 **OBS!** Om du inte trycker på **F10** vid rätt tillfälle, måste du stänga av datorn, starta om den och trycka på **F10** innan operativsystemet startar på datorn för att komma åt programmet.

6. Gå till **Avancerat > PCI-enheter** för att inaktivera både PATA- och SATA-styrenheterna. Lägg märke till vilken IRQ styrenheten har när du inaktiverar SATA-styrningen. Du kommer att behöva göra om IRQ-tilldelningen senare. Avsluta inställningar, och bekräfta ändringarna.

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

7. Sätt i en startbar DOS-diskett med FDISK.COM och antingen SYS.COM eller FORMAT.COM i en diskettenhet och sätt på datorn så att den startar upp från DOS-disketten.
8. Kör FDISK och radera alla eventuella partitioner på USB-flashmediaenheten. Skapa en ny partition och markera den som aktiv. Avsluta FDISK genom att trycka på **Esc**.
9. Om inte systemet startar om automatiskt när du avslutar FDISK, trycker du på **Ctrl+Alt+Del** för att starta om med DOS-disketten.
10. Vid **A:\**-prompten skriver du `FORMAT C: /S` och trycker på **Retur**. Format-kommandot formaterar USB-flashmediaenheten, lägger till systemfilerna och ber dig ange en volymetikett.
11. Tryck på **Retur** om du inte vill ange etikett eller ange, om du så önskar, en etikett.
12. Stäng av datorn och dra ut nätsladden. Öppna datorn och installera om eventuella PCI-kort som du tog bort tidigare. Sätt tillbaka datorns lock.
13. Sätt i nätsladden, ta ur disketten och starta datorn.
14. Så snart datorn har startat, tryck på snabbtangenter **F10** innan operativsystemet startar på datorn för att komma åt Setup-programmet. Om du vill kan du trycka på **Retur** för att komma förbi titelskärmen.
15. Gå till **Avancerat > PCI-enheter** och aktivera på nytt PATA- och SATA-styrenheterna som inaktiverades i steg 6. Sätt SATA-styrenheten på dess ursprungliga IRQ.
16. Spara ändringarna och avsluta. Datorn startar nu upp från USB-flashmediaenheten som enhet C.

 **OBS!** Den standardmässiga startordningen varierar från dator till dator och kan ändras i setup-programmet (F10). Mer information om datorinställningar finns i *Konfigureringshandbok (F10)*.

Om du har använt en DOS-version från Windows 9x, visas Windows-logon en kort stund. Om du inte vill att den här bilden ska visas, lägger du till en fil med längden noll och namnet LOGO.SYS i rotkatalogen på USB-flashmediaenheten.

Gå tillbaka till [Kopiera till flera datorer på sidan 18](#).

---

## 8 Strömbrytare med två lägen

Med ACPI (Advanced Configuration and Power Interface) kan strömknappen ställas in så att den antingen fungerar som en strömbrytare eller som en vilolägesknapp. Vilolägesfunktionen stänger inte av datorn helt utan är ett viloläge med lägre strömförbrukning. Det gör att du snabbt kan stänga av utan att avsluta program och lika snabbt återgå till samma läge utan förlust av data.

Konfigurera om strömknappen så här:

1. Vänsterklicka på **Start** och välj sedan **Kontrollpanelen > Energialternativ**
2. I **Egenskaper för energialternativ** väljer du fliken **Avancerat**.
3. I avsnittet **Strömknapp** väljer du **Viloläge**.

När du har konfigurerat strömknappen att fungera som en vilolägesknapp trycker du på strömknappen för att placera systemet i ett lågt strömförbrukningsläge (vänteläge). Tryck på knappen igen för att väcka systemet till normalläge. Om du helt vill slå av strömmen till systemet trycker du på knappen och håller den inne i fyra sekunder.

---

△ **VIKTIGT:** Använd inte strömknappen för att stänga av datorn såvida inte systemet har hängt sig. Avstängning med strömknappen utan att operativsystemet först stängts kan skada eller förstöra data på hårddisken.

---

---

## 9 HP:S webbplats för Support

HP utför noggranna tester och felsöker program som utvecklats av HP och tredjepartsleverantörer, och utvecklar dessutom hjälpprogram som integreras med operativsystemet för att ge högsta möjliga prestanda, kompatibilitet och tillförlitlighet för HP-datorerna.

Vid övergången till ett nytt eller uppdaterat operativsystem är det viktigt att installera hjälpprogrammen för operativsystemet. Om du tänker köra en version av Microsoft Windows som skiljer sig från den version som levererades med datorn, måste du installera motsvarande drivrutiner och hjälpprogram så att alla funktioner stöds och fungerar som de ska.

HP har gjort det enklare att hitta, komma åt, utvärdera och installera de senaste hjälpprogrammen. Du kan hämta programvara från <http://www.hp.com/support>.

Webbplatsen innehåller de senaste drivrutinerna, hjälpprogrammen och ROM-avbildningarna som behövs för att köra de senaste versionerna av Microsoft Windows operativsystem i din HP-dator.

---

# 10 Industristandarder


HPs hanteringslösningar integreras med andra systemhanteringsprogram och är baserade på industristandarderna såsom:

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

# 11 Inventariekontroll och säkerhet

De inbyggda funktionerna för inventariekontroll ger användaren möjlighet att samla in inventariedata, som kan hanteras av HP Systems Insight Manager, HP Client Manager, HP Configuration Management Solution, HP Client Configuration Manager eller andra systemhanteringsprogram. Eftersom inventariefunktionerna automatiskt och intimt integreras med dessa hanteringsverktyg, kan du använda det verktyg som passar bäst i ditt system och få ut det mesta möjliga av de verktyg som du redan har.

HP erbjuder också flera lösningar för att styra åtkomsten till viktiga komponenter och information. HP Embedded Security for ProtectTools (Inbyggda säkerhetsverktyg), om sådan finns, förhindrar obehörig åtkomst till data och kontrollerar systemets integritet samt kontrollerar den uppgivna identiteten hos tredjepartsanvändare som försöker använda datorn. (Se *HP ProtectTools Security Manager Guide* på <http://www.hp.com/products/security> för mer information.) Säkerhetsfunktioner såsom HP Embedded Security for ProtectTools, Smart Cover Sensor och Smart Cover Lock, som finns på vissa modeller, hjälper till att hindra obehörig åtkomst till datorns interna komponenter. Du kan skydda värdefulla datatillgångar genom att inaktivera parallella eller seriella portar och USB-portar eller genom att inaktivera start från flyttbara media. Larm från Memory Change och Smart Cover Sensor kan skickas automatiskt till systemhanteringsprogram vilket ger en tidig varning om att någon försöker komma åt datorns inre komponenter.

 **OBS!** HP Embedded Security for ProtectTools, Smart Cover Sensor och Smart Cover Lock finns som tillval på vissa system.

Använd följande program för att hantera säkerhetsinställningarna i din HP-dator:

- Lokalt, med hjälp av funktionerna i setup-programmet. Mer information om hur man använder konfigurationsverktyget finns i handboken *Konfigureringshandbok (F10)* som medföljer datorn. Vissa datorer har också HP BIOS Configuration for ProtectTools, vilket är en Windows-baserad komponent i ProtectTools som hjälper administratörer att konfigurera BIOS-säkerhetsinställningar inifrån operativsystemet.
- Fjärrhantering med HP Client Manager från Symantec, HP Client Automation, eller System Software Manager. Dessa program möjliggör säker och enhetlig uppgradering och kontroll av säkerhetsinställningar.

Följande tabell och avsnitt visar lokal hantering av säkerhetsfunktioner i datorn med setup-programmet.

**Tabell 11-1 Säkerhetsfunktioner, översikt**

Funktion	Beskrivning
<b>Setup-lösenord</b>	Ställ in och aktivera lösenordet (administratörs-) för Setup-programmet.  <b>OBS!</b> Om lösenord ställts in måste detta anges för att kunna ändra alternativ i Setup-programmet, uppgradera flash-ROM eller ändra vissa plug&play-inställningar under Windows.
<b>Startlösenord</b>	Du kan ange lösenord för start. Prompten för startlösenordet visas efter en uppstartscykel. Om användaren inte anger korrekt startlösenord, kommer enheten inte att starta.

**Tabell 11-1 Säkerhetsfunktioner, översikt (fortsättning)**

---

**OBS!** Detta lösenord visas inte vid varmstarter, t.ex. via **Ctrl+Alt+Delete** eller **Starta om från Windows**, om inte detta har aktiverats under **Lösenordsalternativ** (se nedan).

---

<b>Lösenordsalternativ</b>	Här kan du: <ul style="list-style-type: none"><li>• Låsa legacy-resurser (visas om ett setup-lösenord är inställt)</li><li>• Aktivera/inaktivera nätverksserverläge (visas om ett startlösenord har ställts in)</li><li>• Ange om lösenordet krävs för omstart (<b>Ctrl+Alt+Delete</b>) (visas om ett startlösenord är inställt)</li><li>• Aktivera/inaktivera installations-blåddringsläge (visas om ett installationslösenord är inställt) (tillåter visning men inte ändring av F10-setupalternativen utan att setup-lösenordet anges)</li><li>• Aktivera/inaktivera Bindande lösenord (visar sig om ett startlösenord är installerat) som när det aktiverats, förbigår den inbyggda lösenordsväxeln för att inaktivera startlösenordet.</li></ul> <p>Mer information finns i avsnittet <i>Skrivbordshanteringsguide</i>.</p>
<b>Smart Cover</b> (vissa modeller)	Här kan du: <ul style="list-style-type: none"><li>• Låsa/låsa upp Cover Lock.</li><li>• Ställa in öppningssensorn till Inaktivera/Meddela användaren/Setup-lösenord.</li></ul> <p><b>OBS!</b> <i>Meddela användare</i> varnar användaren om att sensorn har detekterat att locket har tagits bort. <i>Setup-lösenord</i> gör att setup-lösenord måste anges för att starta datorn om sensorn detekterat att locket tagits bort.</p> <p>Funktionen finns bara på vissa modeller.</p>
<b>Enhetssäkerhet</b>	Gör att du kan ställa in Enhet tillgänglig/Dold enhet för: <ul style="list-style-type: none"><li>• Seriella portar</li><li>• Parallell port</li><li>• Bakre USB-portar</li><li>• Främre USB-portar</li><li>• Interna USB-portar</li><li>• Systemljud</li><li>• Nätverksstyrenheter (vissa modeller)</li><li>• Legacy-diskett</li><li>• Inbyggd säkerhetsanordning (vissa modeller)</li><li>• SATA0</li><li>• SATA1 (vissa modeller)</li><li>• SATA2 (vissa modeller)</li><li>• SATA3 (vissa modeller)</li><li>• eSATA (vissa modeller)</li></ul>
<b>Nätverksservicestart</b>	Aktivera/inaktivera datorns möjlighet att starta från operativsystemet på en nätverksserver. (Funktionen finns bara på NIC-modeller. Nätverkskortet måste vara antingen installerat som ett PCI-kort eller inbyggt i moderkortet.)

---



**Tabell 11-1 Säkerhetsfunktioner, översikt (fortsättning)**

<b>System IDs</b>	Du kan ställa in <ul style="list-style-type: none"><li>• Asset tag (en identifierare, tillgångsnummer, på 18 byte), det inventarienummer datorn fått i företaget.</li><li>• Ownership Tag (Ägarmärkning – en identifierare på 80 byte) visas under POST.</li><li>• Chassits serienummer eller UUID (Universal Unique Identifier). UUID kan uppdateras endast om aktuellt chassiserienummer är ogiltigt. (Dessa nummer ställs normalt in på fabriken och används för att ge systemet en unik identitet.)</li><li>• Tangentbordets nationella inställning (t ex engelskt eller tyskt).</li></ul>
<b>DriveLock-säkerhet</b>	<p>Gör att du kan ange eller ändra ett huvud- eller användarlösenord för hårddiskar. När denna funktion är aktiverad, måste användaren ange ett av DriveLock-lösenorden under POST. Om inget kan anges korrekt kommer hårddisken att vara oåtkomlig tills ett av lösenorden anges korrekt vid följande omstart.</p> <p><b>OBS!</b> Detta alternativ visas bara om minst en hårddisk finns som stöder DriveLock-funktionen finns i systemet.</p>
<b>Systemsäkerhet</b> (vissa modeller: Dessa alternativ är maskinvaruberoende)	<p>Läget Dataexekveringsskydd (vissa modeller) (aktivera/inaktivera) - Hjälper till att förhindra säkerhetsintrång i operativsystemet.</p> <p>Virtualization Technology (vissa modeller) (aktivera/inaktivera) - Styr processorns virtualiseringsfunktioner. Ändring av denna inställning kräver att datorn stängs av och sätts på igen.</p> <p>Virtualization Technology Directed I/O (vissa modeller) (aktivera/inaktivera) - Styr kretsupsättningens DMA-omkopplingsfunktioner för virtualisering. Ändring av denna inställning kräver att datorn stängs av och sätts på igen.</p> <p>Trusted Execution Technology (vissa modeller) (aktivera/inaktivera) - Styr den underliggande processorn och kretsupsättningsfunktioner som krävs för att ge stöd för en virtuell maskin. Ändring av denna inställning kräver att datorn stängs av och sätts på igen. För att aktivera denna funktion måste du aktivera följande funktioner:</p> <ul style="list-style-type: none"><li>• Inbyggt stöd för säkerhetsenhet</li><li>• Virtualiseringsteknologi</li><li>• Virtualiseringsteknologi Directed I/O</li></ul> <p>Inbäddat stöd för säkerhetsenhet (vissa modeller) (aktivera/inaktivera) - Gör att den inbäddade säkerhetsenheten kan aktiveras eller inaktiveras. Ändring av denna inställning kräver att datorn stängs av och sätts på igen.</p> <p><b>OBS!</b> Du måste ange ett lösenord för att kunna konfigurera en inbäddad säkerhetsenhet.</p> <ul style="list-style-type: none"><li>• Återställ fabriksinställningarna (vissa modeller) (Återställ inte/Återställ) - Återställning till fabriksinställningarna raderar alla säkerhetsnycklar. Ändring av denna inställning kräver att datorn stängs av och sätts på igen.</li></ul> <p><b>VIKTIGT:</b> Den inbäddade säkerhetsenheten är en viktig komponent i många säkerhetsschemor. Genom att radera säkerhetsnycklarna förhindras åtkomst till data som skyddas av den inbäddade säkerhetsenheten. En återställning till fabriksinställningar kan resultera i förlust av data.</p> <ul style="list-style-type: none"><li>• Autentiseringsstöd vid start (vissa modeller) (aktivera/inaktivera) - Styr vilket lösenordsautentiseringsschema som använder den inbäddade säkerhetsenheten. Ändring av denna inställning kräver att datorn stängs av och sätts på igen.</li><li>• Återställ autentiseringsinformation (vissa modeller) (Återställ inte/Återställ) - Genom att välja Återställ inaktiveras stödet för autentisering vid start och raderar autentiseringsinformationen från den inbäddade säkerhetsenheten. Ändring av denna inställning kräver att datorn stängs av och sätts på igen.</li></ul>

**Tabell 11-1 Säkerhetsfunktioner, översikt (fortsättning)**

Operativsystemshantering av inbäddad säkerhetsenhet (vissa modeller) (aktivera/inaktivera) - Detta alternativ gör att användaren kan begränsa operativsystemets styrning av den inbäddade säkerhetsenheten. Ändring av denna inställning kräver att datorn stängs av och sätts på igen. Detta alternativ gör att användaren kan begränsa operativsystemets styrning av den inbäddade säkerhetsenheten.

- Återställning av den inbäddade säkerhetsenheten via operativsystemet (vissa modeller) (aktivera/inaktivera) - Detta alternativ gör att användaren kan begränsa operativsystemets möjlighet att begära en fabriksåterställning av den inbäddade säkerhetsenheten. Ändring av denna inställning kräver att datorn stängs av och sätts på igen.

**OBS!** Du måste ange ett lösenord för att kunna aktivera detta alternativ.

BIOS-lösenordstöd för Smart Card (vissa modeller) (aktivera/inaktivera) - Gör att användaren kan aktivera/inaktivera att Smart Card ska användas istället inställnings- och startlösenord. Denna inställning kräver ytterligare initialisering i ProtectTools innan den aktiveras.

PAVP (några modeller) (inaktiverad/min/max) - PAVP aktiverar Protected Audio Video Path i kretsutrustningen. Detta kan ge tillåtelse att visa något av det skyddade högupplösta innehåll som annars skulle vara förbjudet att spela upp Om du väljer Max kommer 96 MB systemminne att tilldelas exklusivt åt PAVP.

---

**Setup-säkerhetsnivå**

Ger en metod för att ge slutanvändare begränsad åtkomst att ändra angivna setup-alternativ utan att känna till setup-lösenordet.

Denna funktion ger administratören flexibiliteten att förhindra ändringar av kritiska setup-alternativ, medan användaren ändå kan tillåtas att se systeminställningar och konfigurera mindre kritiska alternativ. Administratören anger åtkomsträttigheter till enskilda setup-alternativ på en fall-till-fall-basis via menyn Setup-säkerhetsnivå. Som standard är alla setup-alternativ bundna till setup-lösenordet, vilket indikerar att användaren måste ange korrekt setup-lösenord under POST för att kunna göra några ändringar. Administratören kan ställa in enskilda alternativ till Inget, vilket indikerar att användaren kan utföra ändringar på de angivna alternativen även när ett felaktigt setup-lösenord har angetts. Alternativet, Inget, ersätts med startlösenordet om ett sådant är aktiverat.

**OBS!** Setup-bläddringsläget måste ställas in till Aktivera för att användaren ska kunna starta setup-programmet utan att ange setup-lösenordet.

---

## Lösenordsskydd

Startlösenordet hindrar obehörig användning av datorn genom att det måste anges varje gång datorn startas eller startas om för att komma åt program eller data i datorn. Lösenordet för Setup-programmet hindrar obehörig åtkomst av Setup-programmet och kan också användas för att komma förbi lösenordet vid strömpåslag. När du uppmanas att ange startlösenordet kan du i stället ange setup-lösenordet för att kunna använda datorn.


En nätverksinstallation av lösenordet för Setup-programmet kan skapas så att systemadministratören kan logga in i alla system i nätverket och underhålla dem utan att känna till lösenordet vid strömpåslag, även om ett sådant har ställts in.

## Skapa ett setup-lösenord med setup-programmet

Om systemet är utrustat med en inbyggd säkerhetsanordning kan du läsa mer i *HP ProtectTools Security Manager Guide* på <http://www.hp.com>. Om du ställer in ett setup-lösenord med setup-programmet kan inte datorn konfigureras om (med setup-programmet (F10)) förrän lösenordet har angivits.

1. Starta eller starta om datorn. Om du är i Windows klickar du på **Start > Stäng av > Starta om**.
2. Så snart datorn har startat, tryck på snabbtangentsen **F10** innan operativsystemet startar på datorn för att komma åt Setup-programmet. Om du vill kan du trycka på **Retur** för att komma förbi titelskärmen.

---

 **OBS!** Om du inte trycker på **F10** vid rätt tillfälle, måste du stänga av datorn, starta om den och trycka på **F10** innan operativsystemet startar på datorn för att komma åt programmet.

---


3. Välj **Säkerhet** och sedan **Setup-lösenord** och följ instruktionerna på skärmen.
4. Innan du avslutar, sparar du ändringarna genom att klicka på **Arkiv > Spara ändringarna och Avsluta**.

## Skapa ett Start-lösenord med Setup-programmet

Om du skapar ett startlösenord med setup-programmet måste detta lösenord anges när du startar datorn. Om ett startlösenord ställts in visas **Lösenordsalternativ** på menyn **Säkerhet** i setup-programmet. Bland lösenordsalternativen finns också **Lösenord vid omstart**. Om **Lösenord vid omstart** är aktiverat, måste lösenordet anges också varje gång datorn startas om.

1. Starta eller starta om datorn. Om du är i Windows klickar du på **Start > Stäng av > Starta om**.
2. Så snart datorn har startat, tryck på snabbtangentsen **F10** innan operativsystemet startar på datorn för att komma åt Setup-programmet. Om du vill kan du trycka på **Retur** för att komma förbi titelskärmen.

---

 **OBS!** Om du inte trycker på **F10** vid rätt tillfälle, måste du stänga av datorn, starta om den och trycka på **F10** innan operativsystemet startar på datorn för att komma åt programmet.

---

3. Välj **Säkerhet** och sedan **Startlösenord** och följ instruktionerna på skärmen.
4. Innan du avslutar, sparar du ändringarna genom att klicka på **Arkiv > Spara ändringarna och Avsluta**.

## Ange ett startlösenord

Så här anger du ett startlösenord:

1. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start > Stäng av > Starta om datorn**.
2. När nyckelikonen visas på skärmen anger du det aktuella lösenordet och trycker på **Retur**.

---

 **OBS!** Skriv noggrant, av säkerhetsskäl visas inte tecknen som du skriver.

---


Om du anger ett felaktigt lösenord visas en avbruten nyckel. Försök på nytt. Efter tre misslyckade försök måste du slå av datorn och sedan slå på den igen innan du kan fortsätta.

## Ange ett lösenord för Setup-programmet


Om systemet är utrustat med en inbyggd säkerhetsanordning kan du läsa mer i *HP ProtectTools Security Manager Guide* på <http://www.hp.com>.

Om ett setup-lösenord har ställts in för datorn måste detta anges varje gång du vill starta Setup-programmet.

1. Starta eller starta om datorn. Om du är i Windows klickar du på **Start > Stäng av > Starta om**.
2. Så snart datorn har startat, tryck på snabbtangenter **F10** innan operativsystemet startar på datorn för att komma åt Setup-programmet. Om du vill kan du trycka på **Retur** för att komma förbi titelskärmen.

 **OBS!** Om du inte trycker på **F10** vid rätt tillfälle, måste du stänga av datorn, starta om den och trycka på **F10** innan operativsystemet startar på datorn för att komma åt programmet.

3. När nyckelikonen visas på skärmen skriver du lösenordet och trycker på **Retur**.

 **OBS!** Skriv noggrant, av säkerhetsskäl visas inte tecknen som du skriver.


Om du anger ett felaktigt lösenord visas en avbruten nyckel. Försök på nytt. Efter tre misslyckade försök måste du slå av datorn och sedan slå på den igen innan du kan fortsätta.

## Ändra ett start- eller setup-lösenord

Om systemet är utrustat med en inbyggd säkerhetsanordning kan du läsa mer i *HP ProtectTools Security Manager Guide* på <http://www.hp.com>.

1. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start > Stäng av > Starta om datorn**.
2. Gå till steg 3 för att ändra startlösenordet.

Om du vill ändra installationslösenordet, tryck på snabbtangenter **F10** så snart datorn har startat samt innan operativsystemet startar på datorn, för att komma åt Setup-programmet. Om du vill kan du trycka på **Retur** för att komma förbi titelskärmen.


 **OBS!** Om du inte trycker på **F10** vid rätt tillfälle, måste du stänga av datorn, starta om den och trycka på **F10** innan operativsystemet startar på datorn för att komma åt programmet.

3. När nyckelikonen visas skriver du det aktuella lösenordet, ett snedstreck (/) eller annan teckenavgränsare, det nya lösenordet, ett snedstreck (/) eller annan teckenavgränsare och det nya lösenordet igen: `aktuellt lösenord/nytt lösenord/nytt lösenord`

 **OBS!** Skriv noggrant, av säkerhetsskäl visas inte tecknen som du skriver.

4. Tryck på **Retur**.

Det nya lösenordet gäller nästa gång du slår på datorn.

 **OBS!** Se [Avgränsare för nationellt tangentbord på sidan 31](#) för information om olika avgränsartecken. Startlösenordet och setup-lösenordet kan också ändras med hjälp av Alternativ för säkerhet i setup-programmet.


## Ta bort ett start- eller setup-lösenord

Om systemet är utrustat med en inbyggd säkerhetsanordning kan du läsa mer i *HP ProtectTools Security Manager Guide* på <http://www.hp.com>.

1. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start > Stäng av > Starta om datorn**.


2. Gå till steg 3 för att ta bort startlösenordet.

För att ta bort installationslösenordet, måste du trycka på **F10** så snart datorn har startat samt innan operativsystemet startar på datorn, för att komma åt Setup-programmet. Om du vill kan du trycka på **Retur** för att komma förbi titelskärmen.

 **OBS!** Om du inte trycker på **F10** vid rätt tillfälle, måste du stänga av datorn, starta om den och trycka på **F10** innan operativsystemet startar på datorn för att komma åt programmet.

3. När nyckelikonen visas skriver du det aktuella lösenordet följt av ett snedstreck (/) eller alternativ teckenavgränsare: aktuellt lösenord/

4. Tryck på **Retur**.

 **OBS!** Se [Avgränsare för nationellt tangentbord på sidan 31](#) för information om olika avgränsartecken. Startlösenordet och setup-lösenordet kan också ändras med hjälp av Alternativ för säkerhet i setup-programmet.

## Avgränsare för nationellt tangentbord

Alla tangentbord har utformats för att uppfylla landsspecifika krav. Syntax och tecken som används för att ändra eller ta bort lösenord beror på tangentbordet som levererades med datorn.

Avgränsare för nationellt tangentbord					
/	Arabiskt	-	Grekiskt	/	Ryskt
=	Belgiskt	.	Hebreiskt	-	Slovakiskt
-	BHKMSS*	-	Ungerskt	-	Spanskt
/	Brasilianskt	-	Italienskt	/	Svenskt/finskt
/	Kinesiskt	/	Japanskt	-	Schweiziskt
-	Tjeckiskt	/	Koreanskt	/	Taiwanesiskt
-	Danskt	-	Latinamerikanskt	/	Thailändskt
!	Franskt	-	Norskt	.	Turkiskt
é	Fransk-kanadensiskt	-	Polskt	/	Amerikansk-engelskt
-	Tyskt	-	Portugisiskt		

\* För Bosnien-Herzegovina, Kroatien, Montenegro, Serbien och Slovenien

## Radera lösenord

Om du glömmer lösenordet får du inte tillgång till datorn. Instruktioner för att ta bort lösenord finns i handboken *Felsökning*.

Om systemet är utrustat med en inbyggd säkerhetsanordning kan du läsa mer i *HP ProtectTools Security Manager Guide* på <http://www.hp.com>.

## DriveLock

DriveLock är en standardsäkerhetsfunktion som förhindrar obehörig tillgång till data på ATA-hårddiskar. DriveLock har installerats som en utökning av setup-programmet. Den är bara tillgänglig om det finns hårddiskar som stödjer ATA:s uppsättning av säkerhetskommandon. DriveLock är till för HP-kunder där datasäkerheten är av stor vikt. För sådana kunder är kostnader för hårddisk eller förlust av data på den ointressanta jämfört med skada som kan orsakas av obehörig tillgång till hårddiskens innehåll. För att kunna ha denna säkerhetsnivå och fortfarande kunna komma åt data om ett lösenord glöms bort använder HP två lösenord för DriveLock. Ett lösenord är till för, och definieras av systemadministratören och det andra lösenordet är till för, och definieras av användaren. Det finns inget sätt att låsa upp enheten om båda lösenorden glöms bort. När DriveLock används är det därför säkrast att data på enheten också kopieras till företagets informationsystem eller regelbundna säkerhetskopior görs. Om båda lösenorden till DriveLock skulle glömmas bort är hårddisken oanvändbar. För användare som inte passar in i denna kundprofil kan detta vara en oacceptabelt hög risk. För användare som passar in i denna kundprofil kan det vara en rimlig risk att ta för att skydda innehållet på hårddisken.

## Använda DriveLock

När en eller flera hårddiskar som stödjer ATA:s uppsättning med säkerhetskommandon upptäcks, visas DriveLock-alternativet på menyn Säkerhet i setup-programmet. Användaren kan ställa in huvudlösenordet eller sätta på DriveLock. Ett användarlösenord måste anges för att kunna sätta på DriveLock. Eftersom den ursprungliga konfigurationen av DriveLock normalt görs av en systemadministratör måste först ett huvudlösenord ställas in. HP rekommenderar att systemadministratörer ställer in ett huvudlösenord oavsett om DriveLock ska aktiveras eller inte. Detta ger administratören möjlighet att ändra DriveLock-inställningarna om hårddisken senare är låst. När huvudlösenordet väl ställts in kan systemadministratören aktivera DriveLock eller ha den avstängd.

Om en låst hårddisk finns kommer POST att kräva lösenord för att låsa upp den. Om ett startlösenord har ställts in och är samma som användarlösenordet behöver du bara ange lösenordet en gång. Om de är olika måste du även ange ett lösenord för DriveLock. Vid start av datorn kan antingen huvud- eller användarlösenordet användas. Vid en omstart anger du samma lösenord som användes för att låsa upp enheten under den föregående starten. Användaren har två försök att ange rätt lösenord. Om det misslyckas båda gångerna vid en uppstart, kommer POST att fortsätta men data på hårddisken kommer att förbli oåtkomliga. Om inget av försöken lyckas vid en omstart eller en omstart från Windows, kommer POST att stanna och användaren instrueras att stänga av och sätta på strömmen igen.

## DriveLock-program

Säkerhetsfunktionen DriveLock kommer mest till praktiskt användning i en företagsmiljö. Systemadministratören kan ansvara för konfiguration av hårddisken vilket bl a innefattar inställning av huvudlösenord för DriveLock och ett tillfälligt användarlösenord. Om en användare glömmor sitt användarlösenord eller om utrustningen ska användas av en annan anställd kan huvudlösenordet användas för att ändra användarlösenordet så att hårddisken blir åtkomlig.

HP rekommenderar att företagets systemadministratörer som vill aktivera DriveLock också sätter upp regler för hur huvudlösenord ska ställas in och underhållas. Detta för att inte en anställd ska kunna ställa in båda DriveLock-lösenorden och sedan sluta på företaget. I detta fall skulle hårddisken bli oanvändbar och behöva bytas ut. Genom att inte ställa in ett huvudlösenord kan systemadministratören å andra sidan bli uteläst från hårddisken och oförmögen att göra rutinkontroller av otillåten programvara och annan inventarietkontroll samt att utföra support.

För användare med lägre säkerhetskrav rekommenderar HP att DriveLock inte aktiveras. Användare i denna kategori är de som inte vanligtvis har känslig information på sin hårddisk. För dessa är risken att förlora en hårddisk genom att glömma lösenorden mycket allvarigare än den skada som kan uppstå till följd av otillåten hårddiskåtkomst. Tillgång till setup-programmet och DriveLock kan begränsas med setup-lösenordet. Genom att sätta ett setup-lösenord som inte ges till användarna kan systemadministratören hindra användarna från att aktivera DriveLock.

## Smart Cover sensor

Cover Removal Sensor, som finns tillgänglig i vissa modeller, är en kombination av hård- och mjukvaruteknik som kan varna dig när datorhöljet eller sidoplåten har tagits bort. Det finns tre nivåer av skydd, som beskrivs i följande tabell.

**Tabell 11-2 Smart Cover Sensor, skyddsnivåer**

Nivå	Inställning	Beskrivning
Nivå 0	Avaktiverad; inaktiv	Smart Cover Sensor är avaktiverad (standard).
Nivå 1	Notify User	När datorn startas om visas ett meddelande om datorns lock eller sidoplåt har tagits bort.
Nivå 2	Setup-lösenord	När datorn startas om visas ett meddelande om datorns lock eller sidoplåt har tagits bort. Du måste ange setup-lösenordet för att kunna fortsätta.

**OBS!** Dessa inställningar kan ändras med setup-programmet. Mer information finns i *Konfigureringshandbok (F10)*.

## Ange skyddsnivå för SmartCover-sensor

Ange en skyddsnivå för Smart Cover Sensor genom att göra på följande sätt:

1. Starta eller starta om datorn. Om du är i Windows klickar du på **Start > Stäng av > Starta om**.
2. Så snart datorn har startat, tryck på snabbtangenter **F10** innan operativsystemet startar på datorn för att komma åt Setup-programmet. Om du vill kan du trycka på **Retur** för att komma förbi titelskärmen.  
**OBS!** Om du inte trycker på **F10** vid rätt tillfälle, måste du stänga av datorn, starta om den och trycka på **F10** innan operativsystemet startar på datorn för att komma åt programmet.
3. Välj **Säkerhet > Smart Cover > Cover Removal Sensor** och välj önskad säkerhetsnivå.
4. Innan du avslutar, sparar du ändringarna genom att klicka på **Arkiv > Spara ändringarna och Avsluta**.

## Smart Cover Lock

Smart Cover Lock är ett programkontrollerat locklås som finns i vissa HP-datorer. Låset hindrar obehöriga från att komma åt datorns inre komponenter. Datorn levereras med Smart Cover Lock i olåst läge.

△ **VIKTIGT:** För att få maximal låssäkerhet för höljet anger du ett installationslösenord. Installationslösenordet hindrar obehöriga att få tillgång till Setup-programmet.

📄 **OBS!** SmartCoverLock finns som tillval för vissa system.




## Låsa med SmartCoverLock

Om du vill aktivera och låsa med Smart Cover Lock gör du på följande sätt:

1. Starta eller starta om datorn. Om du är i Windows klickar du på **Start > Stäng av > Starta om**.
2. Så snart datorn har startat, tryck på snabbtangentsen **F10** innan operativsystemet startar på datorn för att komma åt Setup-programmet. Om du vill kan du trycka på **Retur** för att komma förbi titelskärmen.

---

 **OBS!** Om du inte trycker på **F10** vid rätt tillfälle, måste du stänga av datorn, starta om den och trycka på **F10** innan operativsystemet startar på datorn för att komma åt programmet.


---

3. Välj **Säkerhet > Smart Cover > Cover Lock > Låsalternativ**.
4. Innan du avslutar, sparar du ändringarna genom att klicka på **Arkiv > Spara ändringarna och Avsluta**.

## Låsa upp SmartCoverLock

1. Starta eller starta om datorn. Om du är i Windows klickar du på **Start > Stäng av > Starta om**.
2. Så snart datorn har startat, tryck på snabbtangentsen **F10** innan operativsystemet startar på datorn för att komma åt Setup-programmet. Om du vill kan du trycka på **Retur** för att komma förbi titelskärmen.

---

 **OBS!** Om du inte trycker på **F10** vid rätt tillfälle, måste du stänga av datorn, starta om den och trycka på **F10** innan operativsystemet startar på datorn för att komma åt programmet.

---

3. Välj **Säkerhet > Smart Cover > Cover Lock > Lås upp**.
4. Innan du avslutar, sparar du ändringarna genom att klicka på **Arkiv > Spara ändringarna och Avsluta**.

## Använd FailSafe-nyckeln på Smart Cover-locket.

Om du aktiverar SmartCoverLock och inte kan ange lösenordet för att inaktivera låset måste du använda SmartCover FailSafe Key för att öppna datorn. Du behöver använda Smart Cover FailSafe Key i följande fall:

- Strömavbrott
- Misslyckad start
- Datorkomponentfel (t ex processor eller nätaggregat)
- Bortglömt lösenord

---

△ **VIKTIGT:** Smart Cover-locks FailSafe-nyckel är ett specialverktyg som levereras av HP. Förebygg problem. Beställ den här nyckeln innan du behöver den genom att kontakta en auktoriserad återförsäljare eller serviceleverantör.

---

Du kan erhålla FailSafe Key på något av följande sätt:

- Kontakta en auktoriserad HP-återförsäljare eller -servicegivare.
- Ring lämpligt nummer som finns angivet i garantin.

Mer information om hur man använder Smart Cover FailSafe Key finns i *Referenshandboken*.


## Kabellåsfäste

På datorns baksida (vissa modeller) finns ett kabellås så att datorn kan låsas fast vid arbetsplatsen.

Anvisningar med bilder finns i *Referenshandboken*.

## Identifikation genom fingeravtryck

Med HPs fingeravtrycksidentifiering behöver du inget lösenord, nätverkssäkerheten förbättras, inloggningsprocessen förenklas och kostnaderna för nätverkshanteringen i företaget minskar. Nu kostar det inte längre så mycket att det bara passar HiTech-företag med höga säkerhetskrav.

 **OBS!** Stöd för fingeravtrycksidentifikation finns i vissa modeller.

---

## Felmeddelande och återställning

Funktionerna för felmeddelanden och återställning kombinerar maskin- och programvaruteknologi för att förhindra förlust av viktig information och minimera antalet oavsiktliga stillestånd.

Om datorn är ansluten till ett nätverk som hanteras av HP Client Manager, skickar datorn också ett felmeddelande till nätverkshanteraren. Med HP Client Manager Software kan du även fjärrplanera diagnostiken så att den körs automatiskt i alla hanterade datorer och skapa en sammanfattningsrapport över misslyckade tester.

## DPS (Drive Protection System)

DPS (Drive Protection System) är ett diagnostiskt verktyg som är förinstallerat på hårddisken i vissa HP-datorer. DPS har utformats för att diagnostisera problem som kan leda till onödiga byten av hårddiskar.


När HP-datorer byggs testas varje hårddisk med DPS och en permanent post med nyckelinformation skrivs till hårddisken. Varje gång DPS körs skrivs testresultatet till hårddisken. En auktoriserad HP-återförsäljare kan använda informationen för att diagnostisera förhållandena som orsakade att DPS-programmet kördes. Anvisningar för hur du använder DPS finns i handboken *Felsökning*.

## Nättaggregat med överspänningskydd

En integrerad strömsprångstolerant strömförsörjning ger större pålitlighet när datorn drabbas av överslag. Strömkällan kan klara strömsprång på upp till 2 000 V utan att systemet går ned eller data förloras.

## Termisk sensor

Temperaturgivaren är en hård- och mjukvarufunktion som spårar datorn interna temperatur. Den här funktionen visar ett varningsmeddelande när det normala intervallet överskrids, vilket ger dig tid att agera innan interna komponenter skadats eller data gått förlorat.

 **VIKTIGT:** Vid hög temperatur kan systemet skadas eller data gå förlorat.

---

# Index

## A

Altiris  
    AClient 3  
    Client Management Suite 10  
    Deployment Solution Agent 3  
ange  
    setup-lösenord 30  
    start-lösenord 29  
avgränsartecken, tabell 31  
avgränsartecken för landsspecifika tangentbord 31

## B

Backup and Recovery Manager 11  
BIOS  
    Boot Block Emergency Recovery Mode 16  
    Fjärruppgradering av flash-ROM 15  
    HPQFlash 15  
Boot Block Emergency Recovery Mode 16

## C

Client Management Interface 5  
Client Manager från Symantec 9

## D

diagnostiskt verktyg för hårddiskar 36  
distributionsverktyg, programvara 2  
DriveLock 32

## F

FailSafe-nyckel, beställa 35  
FailSafe-nyckeln på Smart Cover-locket, beställa 35

Felmeddelande och återställning 36  
fingeravtrycksidentifikation 36  
fjärrinstallation 4  
fjärrinstallation av system 4  
Fjärruppgradering av flash-ROM 15  
Flash-ROM 15  
Förinläst avbildning av programvara 2

## H

Hanteringsteknik 12  
HP  
    Backup and Recovery Manager 11  
    Client Automation Starter, Standard Edition och Enterprise Edition 8  
    Client Catalog för Microsoft System Center- och SMS-produkter 10  
    Client Management Interface 5  
    Client Manager från Symantec 9  
    ProtectTools Security Manager 7  
    System Software Manager 7  
HPQFlash 15  
hårddisk, skydda 36  
hårddiskar, diagnostiskt verktyg 36

## I

indragna lösningar 14  
industristandarder 24  
initial konfiguration 2  
inre temperatur i datorn 36  
Internetadresser. Se webbplatser

inventariespårning 25

## K

kabellås 36  
katastrofåterställningsläge, startblock 16  
kloningsverktyg, programvara 2  
konfiguration av strömbrytare 22  
konfigurera strömknapp 22  
kontrollera åtkomst av datorns komponenter 25

## L

locklås 34  
läsa med Smart Cover Lock 35  
läsa upp med Smart Cover Lock 35  
lösenord  
    på/av 29  
    radera 31  
    setup-program 29, 30  
    säkerhet 28  
    ta bort 31  
    ändra 30

## M

meddelande om ändringar 14

## N

nätaggregat med överspänningsskydd 36

## O

operativsystem, stöd för ändring av 23

## P

Preboot Execution Environment (PXE) 4

Proactive Change Notification (PCN) 14  
 programvara  
   Altiris AClient 3  
   Altiris Client Management Suite 10  
   Altiris Deployment Solution Agent 3  
   distribution 2  
   DPS (Drive Protection System) 36  
   fjärrinstallation av system 4  
   Hanteringsteknik 12  
   HP Backup and Recovery Manager 11  
   HP Client Automation Starter, Standard Edition och Enterprise Edition 8  
   HP Client Catalog för Microsoft System Center- och SMS-produkter 10  
   HP Client Management Interface 5  
   HP Client Manager från Symantec 9  
   HP ProtectTools Security Manager 7  
   HP System Software Manager 7  
   integrering 2  
   inventariespårning 25  
   Proactive Change Notification (PCN) 14  
   uppdatering och hanteringsverktyg 5  
   Verdiem Surveyor 14  
   återställa 2  
 ProtectTools Security Manager 7  
 PXE (Preboot Execution Environment) 4

## R

radera lösenord 31  
 replikera installerade konfigurationer 17

## S

setup  
 initial 2

setup-lösenord  
   ange 30  
   inställning 29  
   ta bort 31  
   ändra 30  
 setup-program  
   kopiera till en enskilda dator 17  
   kopiera till flera datorer 18  
 skydda hårddiskar 36  
 SmartCoverLock  
   låsa 35  
   låsa upp 35  
 Smart Cover Lock 34  
 Smart Cover-lås  
   FailSafe-nyckel 35  
 Smart Cover sensor  
   inställning 34  
   skyddsnivåer 34  
 startbar enhet  
   skapa 19  
   USB-flashmedieenhet 19  
 startbar USB-flashmedieenhet 19  
 Startbar USB-flashmedieenhet 20  
 start-lösenord  
   ange 29  
   inställning 29  
   ta bort 31  
   ändra 30  
 strömbrytare med två lägen 22  
 strömsprångstolerant  
   strömkälla 36  
 stöd för ändring av operativsystem 23  
 Subscriber's Choice 14  
 System Software Manager 7  
 säkerhet  
   DriveLock 32  
   fingeravtrycksidentifikation 36  
   funktioner, tabell 25  
   inställningar 25  
   kabelås 36  
   lösenord 28  
   ProtectTools Security Manager 7  
   Smart Cover Lock 34  
   Smart Cover sensor 34

## T

ta bort lösenord 31  
 temperatur, inne i datorn 36  
 termisk sensor 36

## V

Verdiem Surveyor 14

## W

webbplatser  
   Altiris Client Management Suite 10  
   BIOS-nedladdning 15  
   fjärruppgradering av flash-ROM 15  
   HP Business PC Security 7  
   HP Client Automation Center 8  
   HP Client Catalog för Microsoft SMS 10  
   HP Client Management Interface 6  
   HP Client Management Solutions 3  
   HP Client Manager från Symantec 9  
   HPQFlash 15  
   HP SoftPak Download Manager 6  
   HP Support 11, 12  
   HP System Software Manager 7  
   Hämtningsbara program och drivrutiner 18  
   Intel vPro-teknik 12  
   Konfigurationshantering 3  
   Proactive Change Notification 14  
   programstöd 23  
   ROM-flash 15  
   Subscriber's Choice 14

## A

återställa, programvara 2  
 återställningsläge, startblock, katastrof 16  
 åtkomst av datorns komponenter, kontrollera 25

## Ä

ändra lösenord 30

