HP ProtectTools
Användarhandbok

Första utgåvan: november 2009

Dokumentartikelnummer: 593308-101

Innehåll

1 Introduktion till säkerhet

HP ProtectTools-funktioner ... 2
Nå viktiga säkerhetsmål ... 3
Skydd mot riktad stöld ... 3
Begränsad åtkomst till känslig information ... 3
Förhindra obehörig åtkomst från interna eller externa platser ... 3
Skapa kraftfulla lösenordsprinciper ... 4
Ytterligare säkerhetselement ... 5
Tilldela säkerhetsroller ... 5
Hantera HP ProtectTools-lösenord ... 5
Skapa ett säkert lösenord ... 7
Backup och återställning av HP ProtectTools autentiseringsuppgifter ... 7

2 Komma igång med installationsguiden

3 HP ProtectTools Security Manager Administrative Console

Öppna Administrative Console ... 11
Använda Administrative Console ... 12

4 Konfigurera systemet

Konfigurera autentisering för datorn ... 14
Inloggningsprincip ... 14
Sessionsprincip ... 14
Inställningar ... 15
Administrera användare ... 16
Specificera enhetsinställningar ... 17
Fingeravtryck ... 17
Smart card-kort ... 17
Ansikte ... 17
Avancerade inställningar ... 18

5 Konfigurera dina program

Fliken General (Allmänt) ... 20

Fliken Applications (Program) 21

6 Administrationsverktyg

Uppdateringar och meddelanden 23

7 HP ProtectTools Security Manager

Öppna HP ProtectTools Security Manager 25
Använda instrumentpanelen i Security Manager 26
Installationsprocedurer 27
Registrera autentiseringsuppgifter 27
Registrera fingeravtryck 27
Registrera scener 27
Avancerade användarinställningar 29
Ändra Windows-lösenordet 29
Konfigurera ett smart card-kort 30
Allmänna uppgifter 31
Password Manager 31
För webbsidor eller program där en inloggning ännu inte har skapats 31
För webbsidor eller program där en inloggning redan har skapats 32
Lägga till inloggningar 32
Redigera inloggningar 33
Använda inloggningsmenyn 33
Organisera inloggningar i kategorier 34
Hantera inloggningar 34
Bedöma lösenordets säkerhet 35
Password Managers ikoninställningar 35
Inställningar 36
Credentials (Autentiseringsuppgifter) 36
Ditt personliga ID-kort 37
Göra egna inställningar 37
General 37
Fingerprint (Fingeravtryck) 38
Säkerhetskopiera och återställa data 38
Discover more (Upptäck mer) 39
Uppdateringar och meddelanden 39
Säkerhetsprogram, status 39

8 Drive Encryption för HP ProtectTools (endast vissa modeller)

Installation 41
Öppna Drive Encryption 41
Allmänna uppgifter 42
Aktivera Drive Encryption 42
Inaktivera Drive Encryption 42

Logga in efter aktivering av Drive Encryption 42
Skydda data genom att kryptera hårddisken 43
Visa krypteringsstatus 43
Avancerade uppgifter 44
Hantera Drive Encryption (administratörsuppgift) 44
Kryptera och dekryptera enskilda enheter 44
Säkerhetskopiering och återställning (administratörsuppgift) 44
Säkerhetskopiera nycklar 44
Utföra en återställning 45

9 Privacy Manager for HP ProtectTools (endast vissa modeller)

Installation 47
Öppna Privacy Manager 47
Hantera Privacy Manager-certifikat 47
Beställa och installera ett Privacy Manager-certifikat 47
Beställa ett Privacy Manager-certifikat 48
Att få ett förtilldelat Privacy Manager Corporate-certifikat 48
Installera ett Privacy Manager-certifikat 48
Visa information om Privacy Manager-certifikat 49
Förnya ett Privacy Manager-certifikat 49
Ställa in ett förvalt Privacy Manager-certifikat 49
Radera ett Privacy Manager-certifikat 49
Återställa ett Privacy Manager-certifikat 50
Återkalla ditt Privacy Manager-certifikat 50
Hantera betrodda kontakter 51
Lägga till betrodda kontakter 51
Lägga till en betrodd kontakt 51
Lägga till betrodda kontakter med kontakter från Microsoft Outlook 52
Visa information om betrodda kontakter 53
Radera en betrodd kontakt 53
Kontrollera återkallelsestatus för en betrodd kontakt 53
Allmänna uppgifter 54
Använda Privacy Manager i Microsoft Outlook 54
Konfigurera Privacy Manager för Microsoft Outlook 54
Signera och skicka ett e-postmeddelande 55
Försegla och skicka ett e-postmeddelande 55
Visa ett förseglat e-postmeddelande 55
Använda Privacy Manager i ett Microsoft Office 2007-dokument 55
Konfigurera Privacy Manager för Microsoft Office 56
Signera ett Microsoft Office-dokument 56
Lägga till en signaturrad vid signering av ett Microsoft Word- eller Microsoft Excel-dokument 56

Lägga till signatursättare i Microsoft Word- eller Microsoft Excel-dokument ... 57
Lägga till en signatursättares signaturrad ... 57
Kryptera ett Microsoft Office-dokument ... 58
Ta bort kryptering från ett Microsoft Office-dokument ... 58
Skicka ett krypterat Microsoft Office-dokument ... 58
Visa ett signerat Microsoft Office-dokument ... 59
Visa ett krypterat Microsoft Office-dokument ... 59
Använda Privacy Manager i Windows Live Messenger ... 59
Starta chattsession i Privacy Manager ... 60
Konfigurera Privacy Manager för Windows Live Messenger ... 60
Chatta i Privacy Manager Chat-fönstret ... 61
Visa chatthistorik ... 61
Visa alla sessioner ... 62
Visa sessioner för ett visst konto ... 62
Visa ett sessions-ID ... 62
Visa en session ... 63
Sök efter sessioner med specifik text ... 63
Radera en session ... 63
Lägga till eller ta bort kolumner ... 63
Filtrera visade sessioner ... 64
Avancerade uppgifter ... 65
Migrera Privacy Manager-certifikat och betrodda kontakter till en annan dator ... 65
Säkerhetskopiera Privacy Manager-certifikat och betrodda kontakter ... 65
Återställa Privacy Manager-certifikat och betrodda kontakter ... 65
Central administration av Privacy Manager ... 66

10 File Sanitizer for HP ProtectTools

Shredding ... 68
Free space bleaching ... 69
Installation ... 70
Öppna File Sanitizer ... 70
Skapa ett shredding-schema ... 70
Skapa ett schema för free space bleaching ... 71
Välja eller skapa en shredding-profil ... 71
Välja en fördefinierad shredding-profil ... 71
Anpassa en shredding-profil ... 71
Anpassa en profil för simple delete (enkel radering) ... 72
Allmänna uppgifter ... 74
Använda en tangentsekvens för att initiera shredding ... 74
Använda ikonen File Sanitizer ... 75
Manuell shredding på ett objekt ... 75
Manuell shredding på alla markerade objekt ... 75
Manuell aktivering av free space bleaching ... 76

Avbryta shredding eller free space bleaching 76
Visa loggfilerna 76

11 Device Access Manager for HP ProtectTools (endast vissa modeller)
Installationsprocedurer 78
Öppna Device Access Manager 78
Konfigurera enhetsåtkomst 78
Gruppen Enhetsadministratörer 78
Enkel konfiguration 78
Starta bakgrundstjänst 79
Enhetsklasskonfiguration 80
Neka åtkomst för en användare eller grupp 81
Tillåta åtkomst för en användare eller grupp 82
Ta bort åtkomst för en användare eller grupp 82
Tillåta åtkomst till en klass med enheter för en användare i en grupp 83
Tillåta åtkomst till en specifik enhet för en användare i en grupp 83
Återställa konfigurationen 84
Avancerade uppgifter 85
Kontrollera åtkomst till konfigurationsinställningar 85
Tillåta åtkomst för en befintlig grupp eller användare 85
Neka åtkomst för en befintlig grupp eller användare 86
Lägga till en ny grupp eller användare 86
Ta bort åtkomst för grupp eller användare 86
Relaterad dokumentation 86

12 LoJack Pro för HP ProtectTools

13 Felsökning
HP ProtectTools Security Manager 88
Device Access Manager for HP ProtectTools 90
Diverse 92

Ordlista 93

Index 98

1 Introduktion till säkerhet

I programvaran HP ProtectTools Security Manager finns säkerhetsfunktioner som hjälper till att skydda mot obehörig åtkomst till datorn, nätverk och kritiska data. Administration av HP ProtectTools Security Manager ges via funktionen Administrative Console.

Med hjälp av HP ProtectTools Administrative Console kan den lokala administratören utföra följande aktiviteter:

- Aktivera eller inaktivera säkerhetsfunktioner
- Registrera deras fingeravtryck och fingeravtrycken hos andra som använder den här datorn
- Registrera en eller flera scener för ansiktsautentisering
- Ställa in ett smartcard-kort för autentisering
- Specificera obligatoriska autentiseringsuppgifter
- Administrera användare av datorn
- Justera enhetsspecifika parametrar
- Konfigurera installerade Security Manager-program
- Lägga till fler Security Manager-program

Med hjälp av Security Managers instrumentpanel kan vanliga användare utföra följande uppgifter:

- Konfigurera alternativ som en administratör tillhållit
- Tillåta begränsade kontroller i vissa HP ProtectTools-moduler

Beroende på vilken datormodell du har, kan de tillgängliga programvarumodulerna variera.

HP ProtectTools–programvarumoduler kan vara förinstallerade, förinlästa eller nedladdningsbara från HP:s webbplats. Mer information finns på http://www.hp.com.

OBS! Instruktionerna i denna handledning är skrivna utifrån antagandet att du redan har installerat de tillämpbara HP ProtectTools-programvarumodulerna.

HP ProtectTools-funktioner

I följande tabell visas de viktigaste funktionerna i HP ProtectTools-modulerna.

Modul	Nyckelfunktioner
HP ProtectTools Security Manager Administrative Console (för administratörer)	• Ställ in och konfigurera säkerhetsnivåer och säkra inloggningsmetoder med installationsguiden för Security Manager. • Konfigurera alternativ som är dolda för vanliga användare. • Konfigurera Device Access Manager-konfigurationer och användaråtkomst. • Lägg till och ta bort HP ProtectTools-användare och visa användarstatus med hjälp av administratörsverktyg.
HP ProtectTools Security Manager (för vanliga användare)	• Organisera, ställ in och ändra användarnamn och lösenord. • Konfigurera och ändra inloggningsuppgifter för användare, t.ex. Windows-lösenord och Smart Card. • Konfigurera och ändra shredding, bleaching och inställningar i File Sanitizer. • Visa inställningar för Device Access Manager. • Konfigurera inställningar och alternativ för säkerhetskopiering och återställning.
Credential Manager for HP ProtectTools (Password Manager)	• Spara, organisera och skydda namn och lösenord. • Ställ in inloggningsskärmar för webbplatser och program och snabb och säker åtkomst. • Spara användarnamn och lösenord för webbplatser genom att skriva in dem i Password Manager. Nästa gång du besöker webbplatsen fyller Password Manager i och skickar informationen automatiskt. • Skapa starkare lösenord för högre kontosäkerhet. Password Manager fyller i och skickar informationen automatiskt.
Drive Encryption for HP ProtectTools (endast vissa modeller)	• Ger komplett kryptering av alla volymer på hårddisken. • Kräver förstartsautentisering för att man ska kunna dekryptera och komma åt data.
Privacy Manager for HP ProtectTools (endast vissa modeller)	• Använd avancerade inloggningstekniker för att verifiera källa, integritet och säkerhet vid kommunikation med e-post, Microsoft® Office-dokument och snabbmeddelandeprogram.
File Sanitizer for HP ProtectTools	• "Strimla" (shred) digitala objekt (känslig information som programfiler, historik- eller webbrelaterat innehåll eller annan konfidentiell information) i datorn och regelbundet använda funktionen bleaching på hårddisken.
Device Access Manager for HP ProtectTools (endast vissa modeller)	• Låt IT-ansvariga kontrollera åtkomsten till enheter baserat på användarprofiler. • Förhindra att obehöriga användare tar bort data med externa lagringsmedier och att virus förs in i systemet från externa medier. • Tillåt att administratörer inaktiverar åtkomsten till skrivbara enheter för vissa individer eller grupper av användare.

Nå viktiga säkerhetsmål

HP ProtectTools-modulerna kan fungera ihop för att ge lösningar till en rad säkerhetsfrågor, inklusive följande viktiga säkerhetsmål:

- Stöldskydd
- Begränsa åtkomst till känsliga data
- Förhindra obehörig åtkomst från interna eller externa platser
- Skapa starka lösenordspolicies

Skydd mot riktad stöld

Ett exempel på riktad stöld är stöld av en dator som innehåller konfidentiell information och kundinformation vid en flygplats säkerhetskontroll. Följande funktioner skyddar mot riktad stöld:

- Förstartsautentiseringsfunktionen förhindrar, när det är aktiverat, åtkomst av operativsystemet. Se följande procedurer:
  - Security Manager
  - Drive Encryption

Begränsad åtkomst till känslig information

Låt oss anta att en kontrakterad revisor arbetar på plats och har fått datoråtkomst för att granska känslig ekonomisk information. Du vill inte att revisorn ska kunna skriva ut filerna eller spara dem på en lagringsbar enhet som t.ex. en CD. Följande funktion begränsar åtkomsten till information:

- Med Device Access Manager för HP ProtectTools kan IT-chefen begränsa åtkomsten till lagringsbara enheter så att känslig information inte kan skrivas ut eller kopieras från hårddisken till uttagbara medier.

Förhindra obehörig åtkomst från interna eller externa platser

Obehörig åtkomst till en oskyddad företags-PC utgör en mycket stor risk för hela företagets nätverk med t.ex. information från ekonomiavdelningen, en chef eller avdelningen för F&U, och för privat information såsom patientjournaler eller personliga kontouppgifter. Följande funktioner kan förhindra obehörig åtkomst:

- Förstartsautentiseringsfunktionen förhindrar, när det är aktiverat, åtkomst av operativsystemet. Se följande procedurer:
  - Password Manager
  - Drive Encryption
- Password Manager ser till att en obehörig användare inte får tag i lösenord eller åtkomst till lösenordsskyddade program.
- Med Device Access Manager för HP ProtectTools kan IT-chefen begränsa åtkomsten till lagringsbara enheter så att känslig information inte kan kopieras från hårddisken.

- File Sanitizer gör att du kan radera data på ett säkert sätt genom att "strimla" (shred) viktiga filer och mappar eller använda funktionen bleaching på hårddisken (skriva över data som har raderats men som fortfarande kan återställas).
- DriveLock ser till att ingen kan komma åt data även om hårddisken har tagits ut och installerats i ett oskyddat system.

Skapa kraftfulla lösenordsprinciper

Om en bestämmelse träder i kraft som kräver en kraftfull lösenordsprincip för dussintals webbaserade program och databaser, ger Security Manager en skyddad förvaringsplats för lösenord och bekväm, enkel inloggning med Single Sign On.

Ytterligare säkerhetselement

Tilldela säkerhetsroller

När du hanterar datorsäkerhet (särskilt i stora organisationer) är det viktigt att dela upp ansvar och rättigheter för olika typer av administratörer och användare.

OBS! I en liten organisation eller vid enskild användning kan alla dessa roller innehas av en och samma person.

För HP ProtectTools kan säkerhetsansvaren och –rättigheterna delas upp i följande roller:

- Säkerhetsansvarig – Definierar säkerhetsnivån för företaget eller ntäverket och avgör vilka säkerhetsfunktioner som ska distribueras, t ex Java™ Card-kort, biometriska läsare eller USB-kort.

  OBS! Många av funktionerna i HP ProtectTools kan anpassas av den säkerhetsansvarige i samarbete med HP. Mer information finns på HP:s webbplats http://www.hp.com.

- Administrator – Tillämpar och hanterar de säkerhetsfunktioner som definierats av säkerhetsansvarig. Kan också aktivera och inaktivera vissa funktioner. Om säkerhetsansvarig t.ex. har belutat att distribuera Java-kort, kan IT-administratören aktivera Java Card BIOS-säkerhetsläge.

- Användare – Använder säkerhetsfunktionerna. Om t ex säkerhetsansvarig och IT-administratören har aktiverat Java Card-kort för systemet, kan användaren ställa in Java Card-kortets PIN-kod och använda kortet för autentisering.

VIKTIGT: Administratörer uppmuntras att tillämpa "bästa praxis" när det gäller att begränsa slutanvändarnas privilegier och användarnas åtkomst.

Obehöriga användare bör inte ges administratörsprivilegier.

Hantera HP ProtectTools-lösenord

De flesta av funktionerna i HP ProtectTools Security Manager skyddas med lösenord. I följande tabell visas de vanligaste använda lösenorden, programvarumodulen där lösenordet ställts in och lösenordets funktion.

Även de lösenord som är inställda och använda av enbart IT-administratörer visas i denna tabell. Alla övriga lösenord måste ställas in av vanliga användare eller administratörer.

HP ProtectTools-lösenord	Ställs in i följande modul	Funktion
Windows inloggningslösenord	Kontrollpanelen i Windows® eller HP ProtectTools Security Manager	Kan användas för manuell inloggning och autentisering för åtkomst till olika Security Manager-funktioner.
Lösenord till Security Managers säkerhetskopiering och återställning	Security Manager, av enskild användare	Skyddar mot åtkomst till Security Managers säkerhetskopierings- och återställningsfil.
PIN-kod för Java™ Card-kort	Java Card Security	Skyddar mot åtkomst av Java Card-kortets innehåll och autentiserar användare av Java Card-kortet. När PIN-koden för Java Card-kortet används för autentisering vid start, skyddar den också mot åtkomst till hjälpprogrammet Setup och datorns innehåll.

HP ProtectTools-lösenord	Ställs in i följande modul	Funktion
		Autentiserar användare av Drive Encryption om Java Card-kortet är valt.

Skapa ett säkert lösenord

När du skapar lösenord, måste du först följa de villkor som anges av programmet. I allmänhet bör du beakta följande riktlinjer för att hjälpa dig att skapa bra lösenord och minska riskerna att ditt lösenord avslöjas:

- Använd lösenord med fler än 6 tecken, helst fler än 8.
- Blanda stora och små bokstäver i lösenordet.
- Blanda alfanumeriska tecken och inkludera specialtecken och skiljetecken om så är möjligt.
- Ersätt bokstäver i ett nyckelord med specialtecken och siffror. Du kan t ex använda siffran 1 istället för bokstäverna I eller L.
- Kombinera ord från två eller flera språk.
- Dela upp ett ord eller en fras med siffror eller specialtecken i mitten, t ex ”Mary2-2Cat45.”
- Använd inte lösenord som finns i ordlistor.
- Använd inte ditt namn som lösenord, eller någon annan personlig information som födelsedatum, husdjurens namn eller din mammas flicknamn, även om du skriver det baklänges.
- Byt lösenorden med jämna mellanrum. Du kan ändra bara ett par tecken som påbyggnad.
- Om du skriver ner dina lösenord bör du inte förvara dem på en för alla synlig plats nära datorn.
- Spara inte lösenord i en fil, t ex ett e-postmeddelande, i datorn.
- Dela inte konto och avslöja inte ditt lösenord för någon.

Backup och återställning av HP ProtectTools autentiseringsuppgifter

Du kan använda HP ProtectTools funktion för säkerhetskopiering och återställning för att välja och säkerhetskopiera HP ProtectTools autentiseringsuppgifter och -inställningar.

2 Komma igång med installationsguiden

Installationsguiden för HP ProtectTools vägleder dig genom konfigurationen av de vanligaste funktionerna i Security Manager. Det finns dock en uppsjö av ytterligare funktioner, som du når via HP ProtectTools Administrative Console. Samma inställningar som finns i guiden, liksom ytterligare säkerhetsfunktioner, kan konfigureras med konsolen, som nås från Windows® Start-meny. De här inställningarna gäller datorn och alla användare som delar datorn.

1. När du loggar in en vecka efter den första installationen av datorn, eller första gången en användare med administrativa rättigheter drar ett finger över fingeravtryckskläsaren, startar Security Managers installationsguide automatiskt och vägleder dig genom de grundläggande stegen i att konfigurera programmet. En video med instruktioner för hur du installerar datorn startar automatiskt.

   – eller –

   Öppna HP ProtectTools Security Manager från ikonen **Gadget** på Sidpanelen i Windows eller aktivitetsfältsikonen i meddelandefältet längst till höger i aktivitetsfältet.

   

   Färgen i det övre fältet på Gadget-ikonen indikerar något av följande förhållanden:

   - Röd – HP ProtectTools har inte ställts in, eller så har ett fel uppstått i någon av ProtectTools-modulerna.
   - Gul – Gå till sidan Applications Status (Programstatus) i Security Manager för att se vilka ändringar som måste göras.
   - Blå – HP ProtectTools har ställts in och fungerar korrekt.

   OBS! Gadget-ikonen finns inte i Windows XP.

   – eller –

   Klicka på **Start**, **Alla program** och **HP ProtectTools Administrative Console**.

2. Läs välkomsttexten och klicka på **Next** (Nästa).

   OBS! På välkomstskärmen kan du inaktivera ytterligare visning av guiden genom att välja ett av alternativen.

3. Installationsguiden ber dig att verifiera din identitet.

   Skriv ditt Windows-lösenord eller läs av ditt fingeravtryck med fingeravtryckläsaren och klicka på **Nästa**.

   Om du varken har fingeravtryckläsare eller smartcard-kort, uppmanas du att ange ditt Windows-lösenord. I framtiden måste du alltid använda det här lösenordet när autentisering krävs.

   Om du inte har skapat något Windows-lösenord än, uppmanas du att göra det. Du måste ha ett Windows-lösenord för att kunna skydda ditt Windows-konto mot åtkomst från obehöriga och för att kunna använda funktionerna i HP ProtectTools Security Manager.

4. Installationsguiden vägleder dig genom processen med att installera säkerhetsfunktioner som ska gälla alla som använder datorn:

   - Windows-funktionen Inloggningssäkerhet skyddar ditt Windows-konto genom att kräva specifika autentiseringsuppgifter för åtkomst.
   - Drive Encryption skyddar dina data genom att kryptera hårddiskarna så att informationen blir oläslig för dem som saknar behörighet.
   - Pre-Boot Security skyddar datorn genom att förbjuda åtkomst från obehöriga innan Windows startar.

   OBS! Pre-Boot Security är inte tillgängligt om din dators BIOS inte har stöd för det.

   Du aktiverar en säkerhetsfunktion genom att markera motsvarande kryssruta. Ju fler funktioner du markerar, desto säkrare blir datorn.

5. Klicka på **Finish** (Slutför) på den sista sidan i guiden.

   Security Managers instrumentpanel visas.

OBS! Om du inte slutför guiden, kommer den att starta automatiskt ytterligare två gånger. Därefter kan du nå guiden från meddelandet i meddelandefältet längst till höger i Aktivitetsfältet (såvida du inte har inaktiverat det) tills installationen är klar.

3 HP ProtectTools Security Manager Administrative Console

Administration av HP ProtectTools Security Manager ges via Administrative Console.

OBS! Administration av HP ProtectTools kräver administratörsprivilegier.

Konsolen innehåller följande funktioner:

- Aktivera eller inaktivera säkerhetsfunktioner
- Administrera användare av datorn
- Justera enhetsspecifika parametrar
- Konfigurera Security Manager-program
- Lägga till fler Security Manager-program

▲ När du vill använda programmen i HP ProtectTools Security Manager startar du HP ProtectTools Security Manager från Start-menyn eller högerklickar på ikonen Security Manager i meddelandefältet längst till höger i Aktivitetsfältet.

HP ProtectTools Administrative Console och dess program är tillgängliga för alla användare som delar den här datorn.

Öppna Administrative Console

För administratörsaktiviteter, t.ex. att ställa in systemprinciper eller konfigurera programvara, ska du öppna konsolen så här:

- Klicka på **Start**, **Alla program**, **HP** och **HP ProtectTools Administrative Console**.

  – eller –

  Klicka på **Administration** i den vänstra rutan på Security Managers instrumentpanel.

För användaraktiviteter som t.ex. registrering av fingeravtryck eller användning av Security Manager, öppnar du konsolen så här:

- Klicka på **Start**, **Alla program**, **HP** och **HP ProtectTools Security Manager**.

  – eller –

  Dubbelklicka på ikonen **HP ProtectTools Security Manager** i meddelandefältet längst till höger i Aktivitetsfältet.

Använda Administrative Console

Security Manager Administrative Console är den centrala platsen för administrering av HP ProtectTools Security Manager.

Konsolen består av följande komponenter:

- **Tools** (Verktyg) – Visar följande kategorier för konfigurering av säkerhet i datorn:
  - **Home** (Hem) – Här väljer du vilka säkerhetsaktiviteter som ska utföras.
  - **System** – Här konfigurerar du säkerhetsfunktioner och autentisering för användare och enheter.
  - **Applications** (Program) – Visar generella inställningar för HP ProtectTools Security Managers och Security Managers program.
  - **Data** – Ger en utökad meny med länkar till Security Managers program för dataskydd.
- **Management Tools** (Administrationsverktyg) – Ger information om ytterligare verktyg. Panelen visar följande alternativ:
  - **HP ProtectTools Security Manager Setup Wizard** (Installationsguide för HP ProtectTools Security Manager) – Vägleder dig genom installationen av HP ProtectTools Security Manager.
  - **Help** (Hjälp) – Visar den här hjälpfilen, som ger information om Security Manager och dess förinstallerade program. Hjälpavsnitt för program som du eventuellt lägger till själv finns i de programmen.
  - **About** (Om) – Visar information om HP ProtectTools Security Manager, t.ex. versionsnummer och upphovsrättsinformation.
- **Main area** (Huvudområde) – Visar programspecifika skärmbilder.

4 Konfigurera systemet

Gruppen System når du från menypanelen Tools (Verktyg) till vänster på skärmen i HP ProtectTools Administrative Console. Du kan använda programmen i den här gruppen för att administrera principerna och inställningarna för datorn och dess användare och enheter.

Följande program ingår i gruppen System:

- **Security** (Säkerhet) – Administrera funktioner, autentisering och inställningar som styr hur användarna arbetar med den här datorn.
- **Users** (Användare) – Konfigurera, administrera och registrera användare av den här datorn.
- **Devices** (Enheter) – Administrera inställningar för säkerhetsenheter som är inbyggda i eller anslutna till datorn.

Konfigurera autentisering för datorn

Inom programmet Authentication (Autentisering) kan du välja vilka säkerhetsfunktioner som ska implementeras på den här datorn, ställa in principer som ska styra åtkomsten till datorn och konfigurera ytterligare avancerade inställningar. Du kan specificera de autentiseringsuppgifter som ska krävas för varje klass med användare när du loggar in i Windows eller på webbplatser och program under en användares session.

Så här konfigurerar du autentisering i datorn:

1. Klicka på **Authentication** (Autentisering) på panelmenyn Security (Säkerhet).
2. Konfigurera inloggningsautentisering: Klicka på fliken **Logon Policy** (Inloggningsprincip), gör dina ändringar och klicka på **Apply** (Verkställ).
3. Konfigurera sessionsautentisering: Klicka på fliken **Session Policy** (Sessionsprincip), gör dina ändringar och klicka på **Apply** (Verkställ).

Inloggningsprincip

Så här definierar du principer som styr vilka autentiseringsuppgifter som ska krävas för en användare som loggar in i Windows:

1. Klicka på **Security** (Säkerhet) på menyn Tools (Verktyg) och klicka sedan på **Authentication** (Autentisering).
2. Klicka på en användarkategori på fliken **Logon Policy** (Inloggningsprincip).
3. Specificera vilka autentiseringsuppgifter som ska krävas för den valda användarkategorin. Du måste specificera minst en autentiseringsuppgift.
4. Välj om NÅGON (bara en) av de specificerade autentiseringsuppgifterna ska krävas eller om ALLA specificerade autentiseringsuppgifter ska krävas för en användare. Du kan också stoppa en användare från att komma åt datorn.
5. Klicka på **Apply** (Verkställ).

Sessionsprincip

Så här definierar du principer som styr vilka autentiseringsuppgifter som ska krävas för åtkomst till HP ProtectTools program under en Windows-session:

1. Klicka på **Security** (Säkerhet) på menyn Tools (Verktyg) och klicka sedan på **Authentication** (Autentisering).
2. Klicka på en användarkategori på fliken **Session Policy** (Sessionsprincip).
3. Specificera vilka autentiseringsuppgifter som ska krävas för den valda användarkategorin.
4. Välj om EN av de angivna autentiseringsuppgifterna ska krävas, eller om ALLA av de angivna autentiseringsuppgifterna ska krävas för autentisering av en användare. Du kan också välja att ingen autentisering ska krävas för åtkomst till HP ProtectTools-programmet.
5. Klicka på **Apply** (Verkställ).

Inställningar

Du kan tillåta en eller flera av följande säkerhetsinställningar:

- **Allow One Step logon** (Tillåt enstegsinloggning) – Låter användare av den här datorn hoppa över Windows inloggning om autentisering har utförts på BIOS-nivå eller en nivå med krypterad disk.
- **Allow HP SpareKey authentication for Windows logon** (Tillåt HP SpareKey-autentisering för Windows-inloggning) – Låter användare av den här datorn använda HP SpareKey-funktionen för att logga in i Windows även om det finns andra autentiseringsprinciper som krävs av Security Manager.

Så här redigerar du inställningarna:

1. Klicka när du vill aktivera eller inaktivera en specifik inställning.
2. Klicka på **Apply** (Verkställ) när du vill spara de ändringar du har gjort.

Administrera användare

I programmet Users (Användare) kan du övervaka och administrera den här datorns HP ProtectTools-användare.

Alla HP ProtectTools-användare räknas upp och verifieras mot de principer som ställts in via Security Manager. Dessutom kontrolleras det om de har registrerat rätt autentiseringsuppgifter som gör att de kan följa dessa principer.

När du administrerar användare väljer du bland följande inställningar:

- Lägg till fler användare genom att klicka på **Add** (Lägg till).
- Radera en användare genom att klicka på användaren och sedan på **Delete** (Radera).
- Registrera fingeravtryck eller ställ in fler autentiseringsuppgifter för användaren genom att klicka på användaren och sedan på **Enroll** (Registrera).
- Visa inställningarna för en specifik användare genom att markera användaren, varpå inställningarna visas i det nedre fönstret.

Specificera enhetsinställningar

I programmet Device (Enhet) kan du specificera inställningar som är tillgängliga för alla inbyggda eller anslutna säkerhetsenheter som kan identifieras av HP ProtectTools Security Manager.

Fingeravtryck

På sidan Fingerprints (Fingeravtryck) finns det tre flikar: Enrollment (Registrering), Sensitivity (Känslighet) och Advanced (Avancerat).

Enrollment (Registrering)

Du kan välja det minsta och högsta antal fingeravtryck som en användare får registrera.

Du kan också tömma alla data från fingeravtryckläsaren.

△ **VIKTIGT:** Om du tar bort alla data från fingeravtryckläsaren raderas alla fingeravtrycksdata för alla användare, även administratörer. Om inloggningspolicyn kräver enbart fingeravtryck, kan alla användare då förhindras att logga in på datorn.

Sensitivity (Känslighet)

Du justerar fingeravtryckläsarens känslighet för skanning av fingeravtryck med hjälp av reglaget.

Om ditt fingeravtryck inte identifieras konsekvent, kanske du måste ställa in lägre känslighet. En högre inställning ökar känsligheten för variationer i fingeravtrycksskanningarna och ökar därför risken för falsk acceptans. Inställningen Medium-High (Medel-hög) ger en bra blandning av säkerhet och bekvämlighet.

Advanced (Avancerat)

Du kan konfigurera fingeravtryckläsaren så att den sparar ström när datorn körs på batteri.

Smart card-kort

Du kan konfigurera datorn så att den automatiskt låser sig om ett smart card-kort tas ut. Datorn låser sig dock bara om smart card-kortet har använts som autentiseringsuppgift för inloggning i Windows. Den låser sig inte om du tar ut ett smart card-kort som inte använts för inloggning i Windows.

▲ Markera kryssrutan när du vill aktivera eller inaktivera låsning av datorn när smart card-kortet tas ut.

Ansikte

Du kan ställa in säkerhetsnivån för ansiktsidentifiering så att du får en balans mellan enkel användning och svårighet att ta sig igenom datorns säkerhet.

1. Klicka på **Start**, **Alla program**, **HP** och **HP ProtectTools Administrative Console**.
2. Klicka på **Devices** (Enheter) och sedan på **Face** (Ansikte).

3. Du kan också klicka på reglaget så att det flyttas åt vänster eller, för större precision, klicka på reglaget så att det flyttas åt höger.

   - **Convenience** (Komfort) – För att göra det lättare för registrerade användare att få åtkomst i gränsfall klickar du på skjutreglaget och flyttar det till läget **Convenience** (Komfort).
   - **Balance** (Balans) – Om du vill ha en bra kompromiss mellan säkerhet och enkel användning, eller om du har känslig information eller datorn finns på en plats där obehöriga kan göra försök att logga in, ska du klicka på skjutreglaget så att det flyttas till läget **Balance** (Balans).
   - **Accuracy** (Precision) – Du kan göra det svårare för en användare att få åtkomst om registrerade scener eller de nuvarande ljusförhållandena ligger under normala värden och det är mindre troligt att falsk acceptans uppstår. Klicka på skjutreglaget så att det flyttas till läget **Accuracy** (Precision).

   OBS! Säkerhetsnivån gäller alla användare

4. Klicka på **Apply** (Verkställ).

Avancerade inställningar

1. Klicka på **Start**, **Alla program**, **HP** och **HP ProtectTools Administrative Console**.
2. Klicka på **Devices** (Enheter) och sedan på **Face** (Ansikte).
3. Klicka på **Advanced** (Avancerat).

   - **Do not require user name for Windows logon (Kräv inget användarnamn för Windows-inloggning).**
     - Markera kryssrutan om du vill att användarna ska kunna logga in i Windows utan användarnamn.
     - Avmarkera kryssrutan om du vill att ett användarnamn ska krävas vid inloggning.
   - **Enforce the use of PIN for face logon** (Kräv PIN-kod för ansiktsinloggning) – Markera kryssrutan om du vill att varje användare ska skapa och använda en PIN-kod (personal identification number) vid inloggning.
     - **Minimum length allowed for PIN** (Minimilängd för PIN-kod) – Klicka på uppåtpilen när du vill öka det minsta antalet tecken som krävs för PIN-koden och på nedåpilen när du vill minska det.
     - **Maximum length allowed for PIN** (Maximilängd för PIN-kod) – Klicka på uppåtpilen när du vill öka det maximala antalet tillåtna tecken för PIN-koden och på nedåpilen när du vill minska det.
     - **Maximum retries allowed for PIN** (Största antal försök för PIN-kod) – Klicka på uppåtpilen när du vill öka det maximala antalet gånger som PIN-koden kan anges igen och på nedåtpilen när du vill minska det.

4. Klicka på **OK**.

5 Konfigurera dina program

Gruppen Applications (Program) når du från menypanelen Security Applications (Säkerhetsprogram) till vänster i HP ProtectTools Administrative Console. Du kan använda Settings (Inställningar) för att anpassa funktionen hos de installerade programmen i HP ProtectTools Security Manager.

Så här redigerar du dina programinställningar:

1. Gå till menyn Tools (Verktyg) och klicka på **Settings** (Inställningar) i gruppen **Applications** (Program).
2. Klicka när du vill aktivera eller inaktivera en specifik inställning.
3. Klicka på **Apply** (Verkställ) när du vill spara de ändringar du har gjort.

Fliken General (Allmänt)

Följande inställningar finns på fliken General (Allmänt):

- **Do not automatically launch the Setup Wizard for administrators** (Starta inte Setup Wizard automatiskt för administratörer) – Välj det här alternativet när du vill förhindra att guiden öppnas vid inloggning automatiskt.
- **Do not automatically launch the Getting Started wizard for users** (Starta inte Getting Started Wizard automatiskt för användare) – Välj det här alternativet när du vill förhindra att programmet för användarkonfigurering öppnas automatiskt vid inloggning.

Fliken Applications (Program)

De inställningar som visas här kan ändras när nya program läggs till i Security Manager. Minst följande inställningar visas som standard:

- **Applications status** (Programstatus) – Statusen visas för alla program.
- **Password Manager** (Lösenordshanteraren) – Alla användare av datorn kan använda programmet Password Manager.
- **Privacy Manager** (Sekretesshanteraren) – Alla användare av datorn kan använda programmet Privacy Manager.
- **Enable the Discover more button** (Aktivera knappen Upptäck mer) – Alla användare av den här datorn kan lägga till program i HP ProtectTools Security Manager genom att klicka på knappen **[+] Discover more** ([+] Upptäck mer).

Om du vill återställa alla program till deras fabriksinställningar, klickar du på knappen **Restore Defaults** (Återställ standardvärden).

6 Administrationsverktyg

Det kan finnas ytterligare program som är tillgängliga för att man ska kunna lägga till nya administrationsverktyg i Security Manager. Administratören av den här datorn kan inaktivera funktionen via programmet Settings (Inställningar).

Du lägger till ytterligare administrationsverktyg genom att klicka på **[+] Management tools** (Administrationsverktyg).

Uppdateringar och meddelanden

Om du har en Internet-anslutning kan du gå till DigitalPersonas webbplats http://www.digitalpersona.com/ för att kontrollera om det finns nya program, eller för att upprätta ett schema för automatiska uppdateringar.

1. Om du vill ha information om nya program och uppdateringar, markerar du kryssrutan **Keep me informed about new applications and updates** (Håll mig informerad om nya program och uppdateringar).
2. Om du vill ställa in ett schema för automatiska uppdateringar väljer du önskat antal dagar.
3. Om du vill söka efter uppdateringar klickar du på **Check Now** (Kontrollera nu).

7 HP ProtectTools Security Manager

Med HP ProtectTools Security Manager kan du höja säkerheten i datorn avsevärt.

Du kan använda de förinlästa Security Manager-programmen, liksom ytterligare program som är tillgängliga för omedelbar nedladdning från webben:

- Administrera inloggning och lösenord
- Ändra enkelt ditt lösenord till operativsystemet Windows®
- Göra programinställningar
- Använda fingeravtryck för extra säkerhet och bekvämlighet
- Registrera en eller flera scener för autentisering
- Konfigurera ett smart card-kort för autentisering
- Säkerhetskopiera och återställa programdata
- Lägga till fler program

Öppna HP ProtectTools Security Manager

Du kan öppna HP ProtectTools Security Manager på något av följande sätt:

- Klicka på **Start**, **Alla program**, **HP** och **HP ProtectTools Security Manager**.
- Dubbelklicka på ikonen **HP ProtectTools** i meddelandefältet längst till höger i Aktivitetsfältet.
- Högerklicka på ikonen **HP ProtectTools** och klicka sedan på **Open HP ProtectTools Security Manager** (Öppna HP ProtectTools Security Manager).
- Klicka på gadgeten **Security Manager ID Card** (Security Managers ID-kort) på Sidpanelen i Windows.
- Tryck på snabbtangentkombinationen ctrl+Windows+h så att Security Manager-menyn Quick Links (Snabblänkar) öppnas.

Använda instrumentpanelen i Security Manager

Security Managers instrumentpanel är den centrala punkten för enkel åtkomst till Security Managers funktioner, program och inställningar.

▲ Du öppnar Security Managers instrumentpanel genom att klicka på **Start**, **Alla program**, **HP** och sedan på **HP ProtectTools Security Manager**.

Instrumentpanelen består av följande komponenter:

- **ID Card** (ID-kort) – Visar användarnamnet i Windows och ett valt foto som identifierar den inloggade användaren.
- **Security Applications** (Säkerhetsprogram) – Visar en expanderad meny med länkar för konfigurering av följande säkerhetskategorier:
  - **Credential Manager (Hanteraren för inloggningsuppgifter)**
  - **My Data (Mina data)**
- **Discover more** (Upptäck mer) – Öppnar en sida där du kan hitta fler program som utökar säkerheten för din identitet, information och kommunikation.
- **Main area** (Huvudområde) – Visar programspecifika skärmbilder.
- **Administration** (Administration) – Öppnar HP ProtectTools Administrative Console.
- **Knappen Help** (Hjälp) – Visar information om den aktuella skärmbilden.
- **Advanced** (Avancerat) – Ger åtkomst till följande alternativ:
  - **Preferences** (Inställningar) – Gör att du kan anpassa inställningarna i Security Manager.
  - **Backup and Restore** (Säkerhetskopiering och återställning) – Gör att du kan säkerhetskopiera eller återställa data.
  - **About** (Om) – Visar versionsinformation om Security Manager.

Installationsprocedurer

Registrera autentiseringsuppgifter

Du kan använda sidan My Identity (Min identitet) för att registrera dina olika autentiseringsmetoder, eller autentiseringsuppgifter. När dessa metoder har registrerats, kan du använda dem för att logga in i Security Manager.

Registrera fingeravtryck

Om datorn har en inbyggd eller ansluten fingeravtryckssläsare, får du hjälp av installationsguiden för HP ProtectTools Security Manager med att konfigurera, eller "registrera", dina fingeravtryck.

1. En kontur av två händer visas. Fingrar som redan är registrerade är markerade med grönt. Klicka med ett finger på konturen.

   OBS! Om du vill radera ett fingeravtryck som registrerats tidigare, klickar du på motsvarande finger.

2. När du har valt ett finger att registrera, uppmanas du att läsa in fingret tills fingeravtrycket är registrerat. Ett registrerat finger är markerat med grönt i konturen.

3. Du måste registrera minst två fingrar, helst pekfingret och långfingret. Upprepa steg 1–3 för ett annat finger.

4. Klicka på **Next** (Nästa) och följ sedan instruktionerna på skärmen.

OBS! När du registrerar fingeravtryck med processen i Komma igång, sparas ingen fingeravtrycksinformation förrän du klickar på **Next** (Nästa). Om du lämnar datorn inaktiv en stund, eller om du stänger programmet, sparas dina ändringar **inte**.

Registrera scener

Du måste registrera en eller flera scener för att kunna använda ansiktsinloggning.

Så här registrerar du en ny scen från installationsguiden för HP ProtectTools Security Manager:

1. Klicka på ikonen **HP ProtectTools Security Manager** i sidpanelen till höger på skärmen.

2. Ange ditt Windows®-lösenord och klicka sedan på **Next** (Nästa).

3. Under **Enable security features** (Aktivera säkerhetsfunktioner) markerar du kryssrutan **Windows Logon Security** (Windows Inloggningssäkerhet) och klickar sedan på **Next** (Nästa).

4. Under **Choose your credentials** (Välj dina inloggningsuppgifter) markerar du kryssrutan **Face** (Ansikte) och klickar sedan på **Next** (Nästa).

5. Klicka på **Enroll a new scene** (Registrera ny scen).

När registreringen är klar, kan du också registrera en ny scen om du hade svårigheter under inloggningen därför att ett eller flera av följande villkor hade ändrats:

- Ditt ansikte har förändrats mycket efter den senaste registreringen.
- Belysningen är helt annorlunda än vid alla tidigare registreringar.
- Du bar glasögon (eller inte) under den senaste registreringen.

OBS! Om du har problem med att registrera scener kan du prova med att flytta dig närmare webbkameran. Precis som vid andra typer av fotografering och videoinspelning är belysning och kontrast mycket viktiga. Se till att belysningen främst är i förgrunden och inte i bakgrunden under sessionen. Om Face Recognition (Ansiktsidentifiering) inte autentiserar dig snabbt kan du prova med att registrera om scenen med bättre belysning.

Så här registrerar du en ny scen från HP ProtectTools Security Manager:

1. Klicka på **Start**, **Alla program**, **HP** och **HP ProtectTools Security Manager**.
2. Klicka på **Credentials** (Autentiseringsuppgifter) och sedan på **Face** (Ansikte).
3. Klicka på **Enroll a new scene** (Registrera ny scen).

Avancerade användarinställningar

1. Klicka på **Start**, **Alla program** och **HP ProtectTools Security Manager**.
2. Klicka på **Set up your authentication credentials** (Ställ in dina autentiseringsuppgifter) och sedan på **Face** (Ansikte).
3. Klicka på **Advanced** (Avancerat) och välj sedan bland följande alternativ.

   a. Om du vill att en PIN-kod ska krävas för ansiktsinloggning klickar du på **Create PIN** (Skapa PIN-kod), anger Windows-lösenordet, anger den nya PIN-koden och bekräftar den sedan genom att ange den igen.

   b. Välj ytterligare inställningar om du vill. De här inställningarna gäller bara den aktuella användaren:

   - **Play sound on face recognition events (Spela ett ljud vid händelser med ansiktsidentifiering)**
     - Markera kryssrutan om ett ljud ska spelas när ansiktsidentifieringen går bra eller misslyckas.
     - Avmarkera kryssrutan om du vill inaktivera det här alternativet.
   - **Prompt to update scenes when logon fails (Uppmana till scenuppdatering vid misslyckad inloggning)**
     - Markera kryssrutan om du vill att användaren ska kunna uppdatera scener om ansiktsinloggningen misslyckas. Om verifieringen når tröskelvärdet "maybe" (kanske), uppmanas användaren att bestämma om live-bilderna från den misslyckade inloggningen ska sättas in i den aktuella scenen. Detta kan öka chansen för att inloggningen går bra nästa gång.
     - Avmarkera kryssrutan om du vill inaktivera det här alternativet.
   - **Prompt to enroll a new scene when logon fails (Uppmana till registrering av ny scen vid misslyckad inloggning)**
     - Markera kryssrutan om du vill att användaren ska uppmanas att registrera en ny scen, om ansiktsinloggningen misslyckas och verifieringen inte når tröskelvärdet "maybe" (kanske). Detta kan öka chansen för att inloggningen går bra nästa gång.
     - Avmarkera kryssrutan om du vill inaktivera det här alternativet.

   c. Du registrerar en ny scen genom att klicka på **Enroll a new scene** (Registrera ny scen) och sedan följa instruktionerna på skärmen.

Ändra Windows-lösenordet

Med Security Manager går det lättare och snabbare att ändra Windows-lösenordet än när du gör det med Kontrollpanelen i Windows.

Så här ändrar du Windows-lösenordet:

1. På Security Managers instrumentpanel klickar du på **Credential Manager** (Hanteraren för inloggningsuppgifter) och klickar sedan på **Password** (Lösenord).
2. Ange ditt nuvarande lösenord i textrutan **Current Windows password** (Nuvarande Windows-lösenord).

3. Skriv ett nytt lösenord i textrutan **New Windows password** (Nytt Windows-lösenord) och skriv det sedan en gång till i textrutan **Confirm new password** (Bekräfta nytt lösenord).

4. Klicka på **Change** (Ändra), så ändras ditt nuvarande lösenord omedelbart till det nya.

Konfigurera ett smart card-kort

Om du väljer smartcard-inloggning och datorn har en inbyggd eller ansluten smartcard-läsare, uppmanas du av installationsguiden för Security Manager att skapa en smartcard-PIN-kod (personal identification number).

Så här skapar du en smartcard-PIN-kod:

1. Under **Set up smart card** (Skapa smartcard-kort) anger och bekräftar du en PIN-kod.

   Du kan också ändra din PIN-kod. Ange din nuvarande PIN-kod och sedan en ny.

2. Fortsätt genom att klicka på **Next** (Nästa) och sedan följa instruktionerna på skärmen.

– eller –

▲ På Security Managers instrumentpanel klickar du på **Credentials** (Autentiseringsuppgifter) och klickar sedan på **Smart Card** (Smartcard-kort).

- Så skapar du en smartcard-PIN-kod – Ange och bekräfta en PIN-kod under **Set up smart card** (Skapa smartcard-kort).
- Så här ändrar du en PIN-kod – Ange först din nuvarande PIN-kod och ange och bekräfta sedan en ny.

Allmänna uppgifter

Programmen i den här gruppen hjälper dig att administrera olika aspekter av din digitala identitet.

- **Security Manager** – Skapar och administrerar Quick Links (Snabblänkar), som gör att du kan starta och logga in på webbplatser och program genom autentisering med ditt Windows-lösenord, ditt fingeravtryck eller ett smart card-kort.
- **Credentials** (Autentiseringsuppgifter) – Ett enkelt verktyg när du vill ändra ditt Windows-lösenord, registrera dina fingeravtryck eller konfigurera ett smart card-kort.

Du lägger till fler program genom att klicka på knappen [+] **Discover more** (Upptäck mer) i det nedre vänstra hörnet på instrumentpanelen. Den här knappen kan vara inaktiverad av administratören.

Password Manager

Att logga in i Windows, på webbplatser och i program är enklare och säkrare än någonsin när du använder Password Manager. Du kan använda den för att skapa kraftfullare lösenord som du inte behöver skriva ned eller komma ihåg, och sedan logga in enkelt och snabbt med ett fingeravtryck, ett smart card-kort eller Windows-lösenordet.

Password Manager erbjuder följande alternativ:

- Lägga till, redigera eller ta bort inloggningar från fliken Manage (Administrera).
- Använda Quick Links (Snabblänkar) för att starta standardwebbläsaren och logga in på en webbplats eller ett program, när detta har ställts in.
- Använda dra-och-släpp-teknik för att organisera dina snabblänkar i kategorier.
- Snabbt se om något av dina lösenord är utsatt för en säkerhetsrisk och automatiskt generera ett komplext, kraftfullt lösenord för användning på nya webbplatser.

Många funktioner i Password Manager är också tillgängliga via Password Manager-ikonen, som visas när en webbsida eller en inloggningsskärm för ett program är i fokus. Klicka på ikonen när du vill visa en innehållsmeny där du kan välja bland följande alternativ.

För webbsidor eller program där en inloggning ännu inte har skapats

Följande alternativ visas i innehållsmenyn:

- **Add [somedomain.com] to the Password Manager** (Lägg till [valfrittdomännamn.com] i Password Manager) – Gör att du kan lägga till en inloggning för den nuvarande inloggningsskärmen.
- **Open Password Manager** (Öppna Password Manager) – Startar Password Manager.
- **Icon settings** (Ikoninställningar) – Gör att du kan specificera situationer där Password Manager-ikonen ska visas.
- **Help** (Hjälp) – Visar Password Managers programvaruhjälp.

För webbsidor eller program där en inloggning redan har skapats

Följande alternativ visas i innehållsmenyn:

- **Fill in logon data** (Fyll i inloggningsuppgifter) – Placerar dina inloggningsuppgifter i inloggningsfälten och skickar sedan sidan (om detta specificerades när inloggningen skapades eller då den senast redigerades).
- **Edit logon** (Redigera inloggning) – Gör att du kan redigera dina inloggningsuppgifter för den här webbplatsen.
- **Add a New Account** (Lägg till ett nytt konto) – Gör att du kan lägga till ett konto för inloggning.
- **Open Password Manager** (Öppna Password Manager) – Startar programmet Password Manager.
- **Help** (Hjälp) – Visar Password Managers programvaruhjälp.

OBS! Administratören av den här datorn kan ha ställt in Security Manager så att det kräver mer än en autentiseringsuppgift för att verifiera din identitet.

Lägga till inloggningar

Du kan enkelt lägga till en inloggning för en webbplats eller ett program genom att ange inloggningsinformationen en gång. Därefter fyller Password Manager automatiskt i informationen åt dig. Du kan använda de här inloggningsuppgifterna efter att ha surfat till webbplatsen eller programmet, eller klicka på en inloggning från menyn **Logons** (Inloggningar) så att Password Manager öppnar webbplatsen eller programmet och du loggar in.

Så här lägger du till en inloggning:

1. Öppna inloggningsskärmen för en webbplats eller ett program.
2. Klicka på pilen på **Password Manager**-ikonen och klicka på något av följande, beroende på om inloggningsskärmen är för en webbplats eller ett program:
   - För en webbplats klickar du på **Add [domain name] to Password Manager** (Lägg till [domännamn] i Password Manager).
   - För ett program klickar du på **Add this logon screen to Password Manager** (Lägg till den här inloggningsskärmen i Password Manager).
3. Ange dina inloggningsuppgifter. Inloggningsfälten på skärmen och deras motsvarande fält i dialogrutan identifieras med en kraftig, orangefärgad ram. Du kan också visa den här dialogrutan genom att klicka på **Add Logon** (Lägg till inloggning) från fliken **Password Manager Manage** (Lösenordshanteraren, Hantera). Vissa alternativ är beroende av vilka säkerhetsenheter som är anslutna till datorn; t.ex. om du använder snabbtangenten ctrl+Windows+h, läser in ett fingeravtryck eller sätter i ett smartcard-kort.
   a. Du fyller i ett inloggningsfält med ett av de förformaterade valen genom att klicka på pilarna till höger om fältet.
   b. Lösenordet för den här inloggningen visas om du klickar på **Show password** (Visa lösenord).
   c. Om du vill att inloggningsfälten ska fyllas i utan att skickas, ska du avmarkera kryssrutan **Automatically submit logon data** (Skicka inloggningsuppgifter automatiskt).
   d. Klicka på **OK**, klicka på den autentiseringsmetod du vill använda: **Fingerprints** (Fingeravtryck), **Password** (Lösenord) eller **Face** (Ansikte) och logga sedan in med den valda autentiseringsmetoden.

Plustecknet försvinner från Password Manager-ikonen för att tala om att inloggningen har upprättats.

e. Om Password Manager inte detekterar inloggningsfälten, ska du klicka på **More fields** (Fler fält).

   i. Markera kryssrutan för varje fält som krävs för inloggning, eller avmarkera kryssrutan för fält som inte krävs för inloggning.

   ii. Om Password Manager inte kan detektera alla inloggningsfält, visas ett meddelande som frågar om du vill fortsätta. Klicka på **Yes** (Ja).

   iii. En dialogruta visas med dina inloggningsfält ifyllda. Klicka på ikonen för varje fält och dra den till motsvarande inloggningsfält. Klicka sedan på knappen så att du loggas in på webbplatsen.

   OBS! När du har använt det manuella läget för inmatning av inloggningsdata för en webbplats, måste du fortsätta att använda den här metoden när du vill logga in på samma webbplats i framtiden.

   OBS! Manuell inmatning av inloggningsdata är bara tillgängligt i Internet Explorer 8.

   iv. Klicka på **Close** (Stäng).

Varje gång du går till den webbplatsen eller öppnar det programmet visas Password Manager-ikonen, vilket talar om att du kan använda dina registrerade autentiseringsuppgifter för att logga in.

Redigera inloggningar

Så här redigerar du en inloggning:

1. Öppna inloggningssskärmen för en webbplats eller ett program.
2. Visa en dialogrutan där du kan redigera inloggningsinformationen genom att klicka på pilen på **Password Manager**-ikonen. Klicka sedan på **Edit logon** (Redigera inloggning). Inloggningsfälten på skärmen och deras motsvarande fält i dialogrutan identifieras med en kraftig, orange ram.

   Du kan också visa den här dialogrutan genom att klicka på **Edit for the desired logon** (Redigera önskad inloggning) från fliken **Password Manager Manage** (Hantera Password Manager).
3. Redigera din inloggningsinformation.
   - Du fyller i ett inloggningsfält med något av de förformaterade valen genom att klicka på pilarna till höger om fältet.
   - Om du vill lägga till fler fält från skärmen i din inloggning, ska du klicka på **Fler fält**.
   - Om du vill att inloggningsfälten ska fyllas i utan att skickas, ska du avmarkera kryssrutan **Submit logon data** (Skicka inloggningsuppgifter).
   - Du visar lösenordet för den här inloggningen genom att klicka på **Show password** (Visa lösenord).
4. Klicka på **OK**.

Använda inloggningsmenyn

Password Manager ger ett enkelt och snabbt sätt att starta webbplatser och program som du har skapat inloggningar för. Dubbelklicka på ett programs eller en webbplats inloggning från menyn **Logons**

(Inloggningar) eller fliken **Manage** (Hantera) i **Password Manager**, så öppnas inloggningsskärmen. Fyll sedan i dina inloggningsuppgifter.

När du skapar en inloggning, läggs den automatiskt till på din inloggningsmeny i Password Manager.

Så här visar du inloggningsmenyn:

1. Tryck på snabbtangentskombinationen för **Password Manager**. Fabriksinställningen är ctrl +Windows+h. Du kan ändra snabbtangentskombinationen genom att klicka på **Password Manager** (Lösenordshanteraren) och sedan klicka på **Settings** (Inställningar).
2. Skanna ditt fingeravtryck (på datorer med inbyggd eller ansluten fingeravtrycksläsare).

Organisera inloggningar i kategorier

Använd kategorier när du vill hålla ordning på dina inloggningar genom att skapa en eller flera kategorier. Därefter drar och släpper du inloggningarna i önskade kategorier.

Så här lägger du till en kategori:

1. Från Security Managers instrumentpanel klickar du på **Password Manager**.
2. Klicka på fliken **Manage** (Hantera) och klicka sedan på **Add Category** (Lägg till kategori).
3. Ange ett namn på kategorin.
4. Klicka på **OK**.

Så här lägger du till en inloggning i en kategori:

1. Placera muspekaren över önskad inloggning.
2. Tryck på vänster musknapp och håll ned den.
3. Dra inloggningen till listan med kategorier. Kategorierna markeras allteftersom du drar musen över dem.
4. Släpp musknappen när önskad kategori är markerad.

Dina inloggningar flyttas inte till den valda kategorin, utan kopieras bara dit. Du kan lägga till samma inloggning i mer än en kategori, och du kan visa alla dina inloggningar genom att klicka på **All** (Alla).

Hantera inloggningar

Password Manager gör det enkelt att hantera inloggningsinformationen för användarnamn, lösenord och flera inloggningskonton från en enda, central plats.

Dina inloggningar visas på fliken Manage (Hantera). Om flera inloggningar har skapats för samma webbplats visas varje inloggning under webbplatsens namn med indrag på listan med inloggningar.

Så här hanterar du inloggningar:

På Security Managers instrumentpanel ska du klicka på **Password Manager** och sedan klicka på fliken **Manage** (Hantera).

- **Add a logon** (Lägg till inloggning) – Klicka på **Add Logon** (Lägg till inloggning) och följ instruktionerna på skärmen.
- **Edit a logon** (Redigera en inloggning) – Klicka på en inloggning, klicka på **Edit** (Redigera) och ändra sedan inloggningsuppgifterna.
- **Delete a logon** (Ta bort en inloggning) – Klicka på en inloggning och klicka sedan på **Delete** (Ta bort).

Så här lägger du till ytterligare en inloggning för en webbplats eller ett program:

1. Öppna inloggningsskärmen för webbplatsen eller programmet.
2. Klicka på **Password Manager**-ikonen så att dess genvägsmeny visas.
3. Klicka på **Add additional logon** (Lägg till ytterligare inloggning) och följ instruktionerna på skärmen.

Bedöma lösenordets säkerhet

Det är viktigt att du använder säkra lösenord för inloggning till webbplatser och program så att din identitet skyddas.

Med Password Manager är det lätt att övervaka och förbättra säkerheten med en snabb och automatisk analys av säkerheten i varje lösenord som du annvänder för att logga in på webbplatser och program.

Password Managers ikoninställningar

Password Manager försöker identifiera inloggningsskärmar för webbplatser och program. När den detekterar en inloggningsskärm som du inte har skapat någon inloggning för, uppmanar Password Manager dig att lägga till en inloggning för den skärmen genom att visa Password Manager-ikonen med ett plustecken, "+".

Klicka på ikonpilen och klicka sedan på **Icon Settings** (Ikoninställningar) så att du kan ställa in hur **Password Manager** ska hantera möjliga inloggningsplatser.

- **Prompt to add logons for logon screens** (Uppmana att lägga till inloggningar för inloggningsskärmar) – Klicka på det här alternativet när du vill att Password Manager ska uppmana dig att lägga till en inloggning när en inloggningsskärm som inte har någon inställd inloggning visas.
- **Exclude this screen** (Uteslut den här skärmen) – Markera kryssrutan så att Password Manager inte uppmanar dig en gång till att lägga till en inloggning för den här inloggningsskärmen.

Du når fler av Password Managers inställningar genom att klicka på **Password Manager** och sedan på **Settings** (Inställningar) på Security Managers instrumentpanel.

Inställningar

Du kan specificera inställningar för anpassning av HP ProtectTools Security Manager:

1. **Prompt to add logons for logon screens** (Uppmana att lägga till inloggningar för inloggningsskärmar) – Password Manager-ikonen visas alltid med ett plustecken när en inloggningsskärm för en webbplats eller ett program detekteras, vilket talar om att du kan lägga till en inloggning för den här skärmen i kassaskåpet för lösenord. Du inaktiverar funktionen i dialogrutan **Icon Settings** (Ikoninställningar) genom att avmarkera kryssrutan vid **Prompt to add logons for logon screens** (Uppmana att lägga till inloggningar för inloggningsskärmar).

2. **Open Password Manager with ctrl+Windows+h** (Öppna Password Manager med ctrl+Windows +h) – Standardsnabbtangenten som öppnar Password Managers meny Quick Links (Snabblänkar) är ctrl+Windows+h. Du kan ändra snabbtangenten genom att klicka på det här alternativet och ange en ny tangentkombination. Kombinationer kan bestå av en eller flera av följande tangenter: ctrl, alt eller shift och valfri alfabetisk eller numerisk tangent.

3. Klicka på **Apply** (Verkställ) om du vill spara dina ändringar.

Credentials (Autentiseringsuppgifter)

Du använder dina autentiseringsuppgifter i Security Manager för att verifiera att du verkligen är du. Den lokala administratören av den här datorn kan ställa in vilka autentiseringsuppgifter som kan användas för att bevisa din identitet när du loggar in i ditt Windows-konto, på webbplatser eller i program.

Vilka autentiseringsuppgifter som är tillgängliga kan variera beroende på vilka säkerhetsenheter som är inbyggda i eller anslutna till datorn. Varje autentiseringsuppgift som stöds har en post i gruppen **My Identity, Credentials** (Min identitet, Autentiseringsuppgifter).

Tillgängliga autentiseringsuppgifter, krav och aktuell status visas. Detta kan inbegripa följande:

- Fingeravtryck
- Lösenord
- Smart card-kort
- Ansikte

Du registrerar eller ändrar en autentiseringsuppgift genom att klicka på länken och följa instruktionerna på skärmen.

Ditt personliga ID-kort

Ditt ID-kort identifierar dig som ägare av detta Windows-konto genom att visa ditt namn och en bild som du valt. Det visas tydligt i det övre vänstra hörnet på sidorna i Security Manager och som en gadget på Sidpanelen i Windows.

Att klicka på ID-kortet på Sidpanelen i Windows är ett av många sätt att snabbt få åtkomst till Security Manager.

Du kan ändra bilden och hur ditt namn visas. Som standard visas hela ditt användarnamn i Windows och den bild du valde under Windows-installationen.

Så här byter du visningsnamn:

1. På Security Managers instrumentpanel ska du klicka på ikonen **ID Card** (ID-kort) i det övre vänstra hörnet.
2. Klicka i den kryssruta som visar namnet du angav för ditt konto i Windows. Systemet visar ditt användarnamn i Windows för detta konto.
3. Om du vill ändra namnet skriver du ett nytt namn och klickar sedan på knappen **Save** (Spara).

Så här byter du visningsbild:

1. På Security Managers instrumentpanel ska du klicka på **ID Card** (ID-kort) i det övre vänstra hörnet.
2. Klicka på knappen **Choose picture** (Välj bild), klicka på en bild och klicka sedan på knappen **Save** (Spara).

Göra egna inställningar

Du kan göra egna inställningar av HP ProtectTools Security Manager: På Security Managers instrumentpanel klickar du på **Advanced** (Avancerat) och sedan på **Preferences** (Inställningar). De inställningar som är tillgängliga visas på två flikar: General (Allmänt) och Fingerprint (Fingeravtryck).

General

Följande inställningar finns på fliken General (Allmänt):

Appearance (Utseende) – **Show icon on taskbar** (Visa ikon i Aktivitetsfältet)

- Du aktiverar visning av ikonen i Aktivitetsfältet genom att markera kryssrutan.
- Du inaktiverar visning av ikonen i Aktivitetsfältet genom att avmarkera kryssrutan.

Fingerprint (Fingeravtryck)

Följande inställningar finns på fliken Fingerprint (Fingeravtryck):

- **Quick Actions** (Snabbåtgärder) – Använd den här funktionen när du vill välja vilken Security Manager-aktivitet som ska utföras när du håller ned en definierad tangent medan du läser in ett fingeravtryck.

  Du tilldelar en av de uppräknade tangenterna en snabbåtgärd genom att klicka på ett alternativ med **(tangent) + fingeravtryck** och sedan välja en av de tillgängliga aktiviteterna från menyn.

- **Fingerprint Scan Feedback** (Respons på fingeravtrycksinläsning) – Visas bara när det finns en fingeravtrycksläsare. Använd den här inställningen när du vill justera responsen när du läser in ditt fingeravtryck.

  - **Enable sound feedback** (Aktivera ljudrespons) – Security Manager ger dig respons i form av ett ljud när ett fingeravtryck har lästs in. Olika ljud spelas för olika programhändelser. Du kan tilldela sådana händelser nya ljud på fliken Ljud på Kontrollpanelen i Windows, eller inaktivera ljudresponsen genom att avmarkera det här alternativet.

  - **Show scan quality feedback (Visa respons på inläsningskvalitet)**

    Markera kryssrutan om du vill visa alla inläsningar oavsett kvalitet.

    Avmarkera kryssrutan om du bara vill visa inläsningar av god kvalitet.

Säkerhetskopiera och återställa data

Du bör säkerhetskopiera alla data i Security Manager regelbundet. Hur ofta du ska säkerhetskopiera dem beror på hur ofta de ändras. Om du t.ex. lägger till nya inloggningar dagligen, bör du förmodligen säkerhetskopiera dina data varje dag.

Säkerhetskopior kan också användas vid migrering från en dator till en annan, vilket också kallas att importera och exportera.

OBS! Endast data säkerhetskopieras med den här funktionen.

HP ProtectTools Security Manager måste vara installerat på alla datorer som säkerhetskopierade data ska överföras till innan dessa data kan återställas från filen med säkerhetskopian.

Så här säkerhetskopierar du data:

1. Klicka på **Advanced** (Avancerat) i den vänstra rutan och klicka sedan på **Backup and Restore** (Säkerhetskopiera och återställ).
2. Klicka på **Back up data** (Säkerhetskopiera data).
3. Välj vilka moduler som du vill ta med i säkerhetskopieringen. I de flesta fall bör du välja alla.
4. Ange ett namn på lagringsfilen. Som standard sparas filen i mappen Dokument. Klicka på **Bläddra** om du vill ange en annan plats.
5. Ange ett lösenord som skyddar filen.
6. Verifiera din identitet.
7. Klicka på **Slutför**.

Så här återställer du data:

1. Klicka på **Advanced** (Avancerat) i den vänstra rutan och klicka sedan på **Backup and Restore** (Säkerhetskopiera och återställ).
2. Klicka på **Restore data** (Återställ data).
3. Välj lagringsfilen som du skapade förut. Du kan ange sökvägen i fältet eller klicka på **Browse** (Bläddra).
4. Ange lösenordet som skyddar filen.
5. Välj de moduler vars data du vill återställa. I de flesta fall är detta alla uppräknade moduler.
6. Klicka på **Slutför**.

Discover more (Upptäck mer)

Ytterligare program som ger detta program nya funktioner kan vara tillgängliga.

På Security Managers instrumentpanel klickar du på **[+] Discover more** (Upptäck mer) och bläddra igenom fler program.

OBS! Om det inte finns någon länk som heter **[+] Discover more** (Upptäck mer) i den nedre vänstra delen av instrumentpanelen, har den inaktiverats av datorns administratör.

Uppdateringar och meddelanden

1. Om du vill ha information om nya program och uppdateringar, markerar du kryssrutan **Keep me informed about new applications and updates** (Håll mig informerad om nya program och uppdateringar).
2. Om du vill ställa in ett schema för automatiska uppdateringar väljer du önskat antal dagar.
3. Om du vill söka efter uppdateringar klickar du på **Check Now** (Kontrollera nu).

Säkerhetsprogram, status

Sidan Applications Status (Programstatus) i Security Manager visar den allmänna statusen hos de installerade säkerhetsprogrammen. Sidan visar de program som är installerade och installationsstatusen hos vart och ett. Sammanfattningen visas automatiskt när du öppnar Security Managers instrumentpanel och klickar på **Check the status of the security applications** (Kontrollera statusen hos säkerhetsprogrammen), när du klickar på **Security Applications** (Säkerhetsprogram) och när du klickar på **Check Now** (Kontrollera nu) på **Gadget**-ikonen på sidpanelen i Windows till höger på skärmen.

8 Drive Encryption för HP ProtectTools (endast vissa modeller)

△ **VIKTIGT:** Om du vill avinstallera Drive Encryption-modulen, måste du först dekryptera alla krypterade enheter. Om du inte gör det kommer du inte att komma åt några data i krypterade enheter, såvida du inte har registrerat dig för Drive Encryptions återställningstjänst. Du får inte åtkomst till de krypterade enheterna genom att ominstallera Drive Encryption-modulen.

Drive Encryption for HP ProtectTools ger ett fullständigt dataskydd genom att kryptera datorns hårddisk. När Drive Encryption är aktiverat måste du logga in i Drive Encryptions inloggningsbild, som visas innan operativsystemet Windows® startar.

Med HP ProtectTools Setup Wizard kan Windows-administratörer aktivera Drive Encryption, säkerhetskopiera krypteringsnyckeln, lägga till och ta bort användare och inaktivera Drive Encryption. I HP ProtectTools Security Managers programvaruhjälp finns mer information.

Följande aktiviteter kan utföras med Drive Encryption:

- Krypteringshantering

  Kryptera och dekryptera enskilda enheter

  OBS! Endast interna hårddiskar kan krypteras.

- Återställning
  - Säkerhetskopiera nycklar
  - Utföra en återställning

Installation

Öppna Drive Encryption

1. Klicka på **Start**, **Alla program**, **HP** och **HP ProtectTools Administrative Console**.
2. Klicka på **Drive Encryption** (Enhetskryptering) i den vänstra rutan.

Allmänna uppgifter

Aktivera Drive Encryption

Använd HP ProtectTools Setup Wizard när du vill aktivera Drive Encryption.

OBS! Den här guiden använder man också för att lägga till och ta bort användare.

– eller –

1. Klicka på **Start**, **Alla program**, **HP** och **HP ProtectTools Administrative Console**.
2. Klicka på **Security** (Säkerhet) i den vänstra rutan och klicka sedan på **Features** (Funktioner).
3. Markera kryssrutan **Drive Encryption** (Enhetskryptering) och klicka sedan på **Next** (Nästa).
4. Under **Drives to be encrypted** (Enheter som ska krypteras) markerar du kryssrutan för den hårddisk du vill kryptera.
5. Sätt in lagringsenheten i lämplig plats.

   OBS! Om du vill spara krypteringsnyckeln måste du använda en lagringsenhet av USB-typ med FAT32-format.

6. Under **External storage device on which to save encryption key** (Extern lagringsenhet där krypteringsnyckeln ska sparas) markerar du kryssrutan för den lagringsenhet där krypteringsnyckeln ska sparas.
7. Klicka på **Apply** (Verkställ).

   Enhetskrypteringen börjar.

I HP ProtectTools Security Managers programvaruhjälp finns mer information.

Inaktivera Drive Encryption

Använd HP ProtectTools Setup Wizard när du vill inaktivera Drive Encryption. I HP ProtectTools Security Managers programvaruhjälp finns mer information.

– eller –

1. Klicka på **Start**, **Alla program**, **HP** och **HP ProtectTools Administrative Console**.
2. Klicka på **Security** (Säkerhet) i den vänstra rutan och klicka sedan på **Features** (Funktioner).
3. Avmarkera kryssrutan **Drive Encryption** (Enhetskryptering) och klicka sedan på **Apply** (Verkställ).

   Avkrypteringen av enheten börjar.

Logga in efter aktivering av Drive Encryption

När du startar datorn efter att ha aktiverat Drive Encryption och registrerat ditt användarkonto, måste du logga in i Drive Encryptions inloggningsbild:

OBS! Om Windows-administratören har aktiverat förstartssäkerhet i HP ProtectTools Security Manager, loggas du in på datorn genast när datorn startar istället för att komma till Drive Encryptions inloggningsbild.

1. Klicka på ditt användarnamn och skriv ditt Windows-lösenord eller din Java™ Card-PIN-kod, eller dra ett registrerat finger.
2. Klicka på **OK**.

OBS! Om du använder en återställningsnyckel för att logga in via Drive Encryptions inloggningsbild, blir du också uppmanad att välja ditt användarnamn i Windows och skriva ditt lösenord i Windows inloggningsbild.

Skydda data genom att kryptera hårddisken

Skydda data med HP ProtectTools Setup Wizard genom att kryptera hårddisken:

1. I Security Manager klickar du på **Getting Started** (Komma igång) och klickar sedan på ikonen **Security Manager Setup**. En demonstration som beskriver Security Managers funktioner börjar. (Du kan också starta Security Manager från sidan Drive Encryption (Enhetskryptering).)
2. Klicka på **Drive Encryption** (Enhetskryptering) i vänster ruta och klicka sedan på **Encryption Management** (Krypteringshantering).
3. Klicka på **Change Encryption** (Ändra kryptering).
4. Välj den eller de enheter som ska krypteras.

OBS! Hårddisken bör alltid krypteras.

Visa krypteringsstatus

Användaren kan visa krypteringens status från HP ProtectTools Security Manager.

OBS! Ändringar av enhetskrypteringens status måste göras med HP ProtectTools Administrative Console.

1. Öppna **HP ProtectTools Security Manager**.
2. Under **My Data** (Mina data) klickar du på **Encryption Status** (Krypteringsstatus).

   Om Drive Encryption är aktivt, visar enhetsstatusen en av följande statuskoder:

   - Active (Aktiv)
   - Inactive (Inaktiv)
   - Not encrypted (Okrypterad)
   - Encrypted (Krypterad)
   - Encrypting (Krypterar)
   - Decrypting (Dekrypterar)

   Om hårddisken håller på att krypteras eller dekrypteras, visar en förloppsindikator i procent hur mycket som är klart och hur länge det dröjer innan krypteringen eller dekrypteringen är klar.

Avancerade uppgifter

Hantera Drive Encryption (administratörsuppgift)

På sidan Encryption Management (Krypteringshantering) kan administratörer visa och ändra statusen hos Drive Encryption (aktiv eller inaktiv) och visa krypteringsstatusen hos alla hårddiskar i datorn.

- Om statusen är Inactive (Inaktiv) har Drive Encryption ännu inte aktiverats i HP ProtectTools Security Manager av Windows-administratören och skyddar inte hårddisken. Använd HP ProtectTools Security Manager Setup Wizard när du vill aktivera Drive Encryption.
- Om statusen är Active (Aktiv) har Drive Encryption aktiverats och konfigurerats. Enheten har någon av följande statusar:
  - Not encrypted (Okrypterad)
  - Encrypted (Krypterad)
  - Encrypting (Krypterar)
  - Decrypting (Dekrypterar)

Kryptera och dekryptera enskilda enheter

Du krypterar en eller flera hårddiskar på datorn eller dekrypterar en enhet som redan har krypterats med funktionen Change Encryption (Ändra kryptering):

1. Öppna **HP ProtectTools Administrative Console** och klicka på **Drive Encryption** (Enhetskryptering) och **Encryption Management** (Krypteringshantering).
2. Klicka på **Change Encryption** (Ändra kryptering).
3. I dialogrutan Change Encryption (Ändra kryptering) markerar eller avmarkerar du kryssrutan bredvid varje hårddisk du vill kryptera eller dekryptera. Klicka sedan på **OK**.

OBS! Medan enheten håller på att krypteras eller dekrypteras visar förloppsindikatorn hur länge det dröjer innan processen är klar under den pågående sessionen. Om du stänger av datorn eller initierar strömspar-, vänte- eller viloläge under krypteringen och sedan startar om datorn återställs visningen av den återstående tiden till noll, men den faktiska krypteringen fortsätter där den slutade. Visningen av den återstående tiden och förloppsindikatorn ändras också snabbare för att visa det pågående förloppet.

Säkerhetskopiering och återställning (administratörsuppgift)

På sidan Recovery (Återställning) kan administratörer säkerhetskopiera och återställa krypteringsnycklar.

Local Drive Encryption Key Backup (Säkerhetskopiering av krypteringsnyckel för lokal enhet) – Gör att du kan säkerhetskopiera krypteringsnycklar till uttagbara medier när Drive Encryption är aktiverat.

Säkerhetskopiera nycklar

Du kan säkerhetskopiera krypteringsnyckeln för en krypterade enhet till en uttagbar lagringsenhet:

△ **VIKTIGT:** Förvara lagringsenheten med säkerhetskopian av nyckeln på en säker plats. Om du glömmer lösenordet eller tappar bort ditt Java Card-kort, är denna enhet din enda möjlighet att komma åt hårddisken.

1. Öppna **HP ProtectTools Administrative Console** och klicka på **Drive Encryption** (Enhetskryptering) och **Recovery** (Återställning).
2. Klicka på **Backup Keys** (Säkerhetskopiera nycklar).
3. På sidan Select Backup Disk (Välj disk för säkerhetskopiering) markerar du kryssrutan för den enhet där du vill ha säkerhetskopian av krypteringsnyckeln. Klicka sedan på **Next** (Nästa).
4. Läs informationen på nästa sida som visas och klicka på **Next** (Nästa). Krypteringsnyckeln sparas på den lagringsenhet du valt.
5. Klicka på **Finish** (Slutför) när dialogrutan för bekräftelse visas.

Utföra en återställning

Så här utför du en återställning om du glömmer lösenordet:

1. Starta datorn.
2. Sätt i den flyttbara lagringsenhet som innehåller säkerhetskopian av nyckeln.
3. Klicka på **Cancel** (Avbryt) när dialogrutan för inloggning i Drive Encryption for HP ProtectTools öppnas.
4. Klicka på **Options** (Alternativ) i det nedre vänstra hörnet av skärmen och klicka på **Recovery** (Återställning).
5. Välj den fil som innehåller säkerhetskopian av nyckeln eller klicka på **Browse** (Bläddra) och sök efter den. Klicka sedan på **Next** (Nästa).
6. Klicka på **OK** när dialogrutan för bekräftelse visas.

   Datorn startar.

OBS! Vi rekommenderar att du återställer lösenordet när du har utfört en återställning.

9 Privacy Manager for HP ProtectTools (endast vissa modeller)

Med Privacy Manager for HP ProtectTools kan du använda avancerade metoder för säker inloggning (autentisering) för att verifiera kommunikationens källa, integritet och säkerhet vid användning av e-post, Microsoft® Office-dokument eller snabbmeddelanden.

Privacy Manager bygger på säkerhetsinfrastrukturen i HP ProtectTools Security Manager, med följande metoder för säker inloggning:

- Autentisering med fingeravtryck
- Windows®-lösenord
- HP ProtectTools Java™ Card

Alla dessa metoder för säker inloggning kan användas i Privacy Manager.

Privacy Manager kräver följande:

- HP ProtectTools Security Manager 5.00 eller senare
- Operativsystemet Windows® 7, Windows Vista® eller Windows XP
- Microsoft Outlook 2007 eller Microsoft Outlook 2003
- Ett giltigt e-postkonto

OBS! Ett Privacy Manager-certifikat (ett digitalt certifikat) måste begäras och installeras inifrån Privacy Manager innan du kommer åt säkerhetsfunktionerna. Information om hur du beställer ett Privacy Manager-certifikat finns i Beställa och installera ett Privacy Manager-certifikat på sidan 47.

Installation

Öppna Privacy Manager

Så här öppnar du Privacy Manager:

1. Klicka på **Start**, **Alla program**, **HP** och **HP ProtectTools Security Manager**.
2. Klicka på **Privacy Manager**.

– eller –

Högerklicka på ikonen **HP ProtectTools** i meddelandefältet längst till höger i Aktivitetsfältet, klicka på **Privacy Manager** och klicka sedan på **Konfiguration**.

– eller –

I verktygsfältet i ett e-postmeddelande i Microsoft Outlook klickar du på nedåtpilen bredvid **Send Securely** (Skicka säkert) och sedan på **Certificate** (Certifikat) eller **Trusted Contacts** (Betrodda kontakter).

– eller –

I verktygsfältet i ett Microsoft Office-dokument klickar du på nedåtpilen bredvid **Sign and Encrypt** (Signera och kryptera) och sedan på **Certificate** (Certifikat) eller **Trusted Contact** (Betrodda kontakter).

Hantera Privacy Manager-certifikat

Privacy Manager-certifikat skyddar data och meddelanden med kryptografisk PKI-teknik (public key infrastructure). Med PKI måste användarna skaffa kryptografiska nycklar och ett Privacy Manager-certifikat utfärdat av en certifierande myndighet. Till skillnad från de flesta datakrypterings- och autentiseringsprogram som bara kräver att du autentiserar ibland, kräver Privacy Manager autentisering varje gång du signerar ett e-postmeddelande eller ett Microsoft Office-dokument med en kryptografisk nyckel. Privacy Manager gör processen med att spara och skicka viktig information säker.

Du kan utföra följande aktiviteter:

- Beställa och installera ett Privacy Manager-certifikat
- Visa information om Privacy Manager-certifikat
- Förnya Privacy Manager-certifikat
- När flera certifikat är tillgängliga kan du ställa in att ett standardcertifikat ska användas av Privacy Manager
- Ta bort och återkalla ett Privacy Manager-certifikat (avancerat)

Beställa och installera ett Privacy Manager-certifikat

Innan du kan använda funktionerna i Privacy Manager, måste du beställa och installera ett Privacy Manager-certifikat (i Privacy Manager) genom att använda en giltig e-postadress. E-postadressen måste konfigureras som ett konto i Microsoft Outlook på den dator varifrån du beställer Privacy Manager-certifikatet.

Beställa ett Privacy Manager-certifikat

1. Öppna Privacy Manager och klicka på **Certificates** (Certifikat).
2. Klicka på **Request a Privacy Manager certificate** (Beställ ett Privacy Manager-certifikat).
3. Läs texten på välkomstsidan och klicka på **Next** (Nästa).
4. Läs licensavtalet.
5. Kontrollera att kryssrutan bredvid **Check here to accept the terms of this license agreement** (Markera här om du godkänner villkoren i detta licensavtal) är markerad och klicka på **Next** (Nästa).
6. På sidan Your Certificate Details (Dina certifikatuppgifter) anger du de obligatoriska uppgifterna och klickar på **Next** (Nästa).
7. På sidan Certificate Request Accepted (Certifikatbeställning mottagen) klickar du på **Finish** (Slutför).
8. Klicka på **OK** så att certifikatet stängs.

Du kommer att få ett e-postmeddelande i Microsoft Outlook med ditt Privacy Manager-certifikat som bilaga.

Att få ett förtilldelat Privacy Manager Corporate-certifikat

1. I Outlook öppnar du det e-postmeddelande som du fått och som talar om att ett företagscertifikat har tilldelats dig.
2. Klicka på **Obtain** (Hämta).
3. Du kommer att få ett e-postmeddelande i Microsoft Outlook med ditt Privacy Manager-certifikat som bilaga.
4. Läs om hur du installerar certifikatet i Installera ett Privacy Manager-certifikat på sidan 48

Installera ett Privacy Manager-certifikat

1. När du får e-postmeddelandet med ditt Privacy Manager-certifikat bifogat, ska du öppna e-postmeddelandet och klicka på knappen **Setup** (Installera) i det nedre högra hörnet i meddelandet i Outlook 2007, eller i det övre vänstra hörnet i Outlook 2003.
2. Autentisera dig med önskad metod för säker inloggning.
3. På sidan Certificate Installed (Certifikat installerat) klickar du på **Next** (Nästa).
4. På sidan Certificate Backup (Certifikatkopia) ska du ange plats och namn för filen med säkerhetskopian eller klicka på **Browse** (Bläddra) och sök efter en plats.

   △ **VIKTIGT:** Spara filen någon annanstans än på hårddisken och förvara den säkert. Den här filen bör bara du själv använda. Du behöver den om du måste återställa Privacy Manager-certifikatet och tillhörande nycklar.

5. Ange och bekräfta ett lösenord och klicka sedan på **Next** (Nästa).

6. Autentisera dig med önskad metod för säker inloggning.

7. Om du väljer att påbörja inbjudningsprocessen för betrodda kontakter, följer du anvisningarna på skärmen. Börja med steg 2 i avsnittet Lägga till betrodda kontakter med kontakter från Microsoft Outlook på sidan 52.

   – eller –

   Om du klickar på **Cancel** (Avbryt), bör du läsa i Lägga till en betrodd kontakt på sidan 51 om hur du lägger till en betrodd kontakt senare.

Visa information om Privacy Manager-certifikat

1. Öppna Privacy Manager och klicka på **Certificates** (Certifikat).
2. Klicka på ett Privacy Manager-certifikat.
3. Klicka på **Certificate details** (Certifikatinformation).
4. Klicka på **OK** när du har läst klart.

Förnya ett Privacy Manager-certifikat

När ett Privacy Manager-certifikat börjar närma sig sitt utgångsdatum, får du ett meddelande om att du måste förnya det:

1. Öppna Privacy Manager och klicka på **Certificates** (Certifikat).
2. Klicka på **Renew certificate** (Förnya certifikat).
3. Köp ett nytt Privacy Manager-certifikat enligt anvisningarna på skärmen.

OBS! En förnyelse av ett Privacy Manager-certifikat ersätter inte ditt gamla Privacy Manager-certifikat. Du måste köpa ett nytt Privacy Manager-certifikat och installera det enligt samma procedurer som i Beställa och installera ett Privacy Manager-certifikat på sidan 47.

Ställa in ett förvalt Privacy Manager-certifikat

Det är bara Privacy Manager-certifikat som visas i Privacy Manager, även om ytterligare certifikat från andra certifierande myndigheter är installerade i datorn.

Om du har flera Privacy Manager-certifikat i datorn som har installerats via Privacy Manager, kan du ange att ett av dem ska användas som standard.

1. Öppna Privacy Manager och klicka på **Certificates** (Certifikat).
2. Klicka på det Privacy Manager-certifikat som du vill använda som standard och klicka sedan på **Set default** (Använd som standard).
3. Klicka på **OK**.

OBS! Du behöver inte använda standardcertifikatet i Privacy Manager. Med de olika funktionerna i Privacy Manager kan du välja vilket Privacy Manager-certifikat du vill.

Radera ett Privacy Manager-certifikat

Om du raderar ett Privacy Manager-certifikat, kan du inte öppna några filer eller visa några data som du har krypterat med det certifikatet. Om du oavsiktligt har raderat ett Privacy Manager-certifikat, kan

du återställa det med den säkerhetskopia som du skapade när du installerade certifikatet. Mer information finns i Återställa ett Privacy Manager-certifikat på sidan 50.

Så här raderar du ett Privacy Manager-certifikat:

1. Öppna Privacy Manager och klicka på **Certificates** (Certifikat).
2. Klicka på det Privacy Manager-certifikat du vill radera och klicka sedan på **Advanced** (Avancerat).
3. Klicka på **Delete** (Radera).
4. Klicka på **Yes** (Ja) när dialogrutan för bekräftelse visas.
5. Klicka på **Close** (Stäng) och sedan på **Apply** (Verkställ).

Återställa ett Privacy Manager-certifikat

Under installationen av ditt Privacy Manager-certifikat måste du skapa en säkerhetskopia av certifikatet. Du kan också skapa en säkerhetskopia från migreringssidan. Den här säkerhetskopian kan användas vid migrering till en annan dator och återställning av ett certifikat till samma dator.

1. Öppna Privacy Manager och klicka på **Migration** (Migrering).
2. Klicka på **Restore** (Återställ).
3. Klicka på sidan Migration File (Migrationsfil), klicka på **Browse** (Bläddra) och sök efter .dppsm-filen, som du skapade under säkerhetskopieringen och klicka sedan på **Next** (Nästa).
4. Ange det lösenord du använde när du skapade säkerhetskopian och klicka sedan på **Next** (Nästa).
5. Klicka på **Slutför**.
6. Klicka på **OK**.

Mer information finns i Installera ett Privacy Manager-certifikat på sidan 48 eller Säkerhetskopiera Privacy Manager-certifikat och betrodda kontakter på sidan 65.

Återkalla ditt Privacy Manager-certifikat

Om du misstänker att säkerheten i ditt Privacy Manager-certifikat har försämrats, kan du återkalla ditt eget certifikat:

OBS! Ett återkallat Privacy Manager-certifikat raderas inte. Du kan fortfarande använda det för att visa krypterade filer.

1. Öppna Privacy Manager och klicka på **Certificates** (Certifikat).
2. Klicka på **Advanced** (Avancerat).
3. Klicka på det Privacy Manager-certifikat du vill återkalla och sedan på **Revoke** (Återkalla).
4. Klicka på **Yes** (Ja) när dialogrutan för bekräftelse visas.
5. Autentisera dig med önskad metod för säker inloggning.
6. Följ instruktionerna på skärmen.

Hantera betrodda kontakter

Betrodda kontakter är användare med vilka du har utväxlat Privacy Manager-certifikat för att ni ska kunna kommunicera säkert med varandra.

Med Trusted Contacts Manager kan du utföra följande aktiviteter:

- Visa information om betrodda kontakter
- Ta bort betrodda kontakter
- Kontrollera återkallelsestatus för betrodda kontakter (avancerat)

Lägga till betrodda kontakter

Att lägga till betrodda kontakter är en 3-stegsprocess:

1. Du skickar en inbjudan till en betrodd kontakt via e-post.
2. Den betrodda kontakten svarar på e-postmeddelandet.
3. Du får svaret från den betrodda kontakten och klickar på **Accept** (Godkänn).

Du kan skicka e-postinbjudningar till enskilda mottagare som du vill ha som betrodda kontakter eller till alla kontakter i din adressbok i Microsoft Outlook.

Läs i följande avsnitt om hur du lägger till betrodda kontakter.

OBS! För att kunna svara på din inbjudan att bli betrodd kontakt, måste mottagarna ha Privacy Manager installerat på sina datorer eller ha den alternativa klienten installerad. Information om hur du installerar den alternativa klienten finns på webbplatsen DigitalPersona på http://DigitalPersona.com/PrivacyManager.

Lägga till en betrodd kontakt

1. Öppna Privacy Manager, klicka på **Trusted Contacts Manager** (Hantering av betrodda kontakter) och klicka sedan på **Invite Contacts** (Bjud in kontakter).

   – eller –

   I Microsoft Outlook: Klicka på nedåtpilen bredvid **Send Securely** (Skicka säkert) i verktygsfältet och klicka sedan på **Invite Contacts** (Bjud in kontakter).

2. Om dialogrutan Select Certificate (Välj certifikat) öppnas, klickar du på det Privacy Manager-certifikat du vill använda och sedan på **OK**.

3. När dialogrutan Trusted Contact Invitation (Inbjudan till betrodda kontakter) öppnas, ska du läsa texten och sedan klicka på **OK**.

   Ett e-postmeddelande genereras automatiskt.

4. Ange en eller flera e-postadresser till mottagare som du vill lägga till som betrodda kontakter.

5. Redigera texten och signera med ditt namn (valfritt).

6. Klicka på **Send** (Skicka).

OBS! Om du inte har skaffat något Privacy Manager-certifikat, får du ett meddelande som talar om att du måste ha ett Privacy Manager-certifikat för att kunna bjuda in en betrodd kontakt. Klicka på **OK** så att guiden Certificate Request startar. Mer information finns i Beställa och installera ett Privacy Manager-certifikat på sidan 47.

7. Autentisera dig med önskad metod för säker inloggning.

OBS! När den betrodda kontakten får e-postmeddelandet, måste han eller hon öppna e-postmeddelandet och klicka på **Accept** (Godkänn) i det nedre högra hörnet i e-postmeddelandet och sedan klicka på **OK** när dialogrutan för bekräftelse öppnas.

8. När du får ett e-postsvar från en mottagare som accepterar att bli betrodd kontakt, ska du klicka på **Accept** (Godkänn) i det nedre högra hörnet i e-postmeddelandet.

   En dialogruta öppnas med en bekräftelse på att mottagaren har lagts till i listan med betrodda kontakter.

9. Klicka på **OK**.

Lägga till betrodda kontakter med kontakter från Microsoft Outlook

1. Öppna Privacy Manager, klicka på **Trusted Contacts Manager** (Hantering av betrodda kontakter) och klicka sedan på **Invite Contacts** (Bjud in kontakter).

   – eller –

   I Microsoft Outlook: Klicka på nedåtpilen bredvid **Send Securely** (Skicka säkert) i verktygsfältet och klicka sedan på **Invite All My Outlook Contacts** (Bjud in alla mina Outlook-kontakter).

2. När sidan Trusted Contact Invitation (Inbjudan till betrodda kontakter) öppnas, väljer du e-postadressen till de mottagare du vill lägga till som betrodda kontakter och klickar på **Next** (Nästa).

3. När sidan Sending Invitation (Skickar inbjudan) öppnas, klickar du på **Finish** (Slutför).

   Ett e-postmeddelande innehållande de valda e-postadresserna i Microsoft Outlook genereras automatiskt.

4. Redigera texten och signera med ditt namn (valfritt).

5. Klicka på **Send** (Skicka).

OBS! Om du inte har skaffat något Privacy Manager-certifikat, får du ett meddelande som talar om att du måste ha ett Privacy Manager-certifikat för att kunna bjuda in en betrodd kontakt. Klicka på **OK** så att guiden Certificate Request startar. Mer information finns i Beställa och installera ett Privacy Manager-certifikat på sidan 47.

6. Autentisera dig med önskad metod för säker inloggning.

OBS! När den betrodda kontakten får e-postmeddelandet, måste han eller hon öppna e-postmeddelandet och klicka på **Accept** (Godkänn) i det nedre högra hörnet i e-postmeddelandet och sedan klicka på **OK** när dialogrutan för bekräftelse öppnas.

7. När du får ett e-postsvar från en mottagare som accepterar att bli betrodd kontakt, ska du klicka på **Accept** (Godkänn) i det nedre högra hörnet i e-postmeddelandet.

   En dialogruta öppnas med en bekräftelse på att mottagaren har lagts till i listan med betrodda kontakter.

8. Klicka på **OK**.

Visa information om betrodda kontakter

1. Öppna Privacy Manager och klicka på **Trusted Contacts** (Betrodda kontakter).
2. Klicka på en betrodd kontakt.
3. Klicka på **Contact details** (Kontaktinformation).
4. Klicka på **OK** när du har läst klart.

Radera en betrodd kontakt

1. Öppna Privacy Manager och klicka på **Trusted Contacts** (Betrodda kontakter).
2. Klicka på den betrodda kontakt du vill radera.
3. Klicka på **Delete contact** (Radera kontakt).
4. Klicka på **Yes** (Ja) när dialogrutan för bekräftelse visas.

Kontrollera återkallelsestatus för en betrodd kontakt

Så här kan du se om en betrodd kontakt har återkallat sitt Privacy Manager-certifikat:

1. Öppna Privacy Manager och klicka på **Trusted Contacts** (Betrodda kontakter).
2. Klicka på en betrodd kontakt.
3. Klicka på knappen **Advanced** (Avancerat).

   Dialogrutan Advanced Trusted Contact Management (Avancerad hantering av betrodda kontakter) öppnas.
4. Klicka på **Check Revocation** (Kontrollera återkallelse).
5. Klicka på **Stäng**.

Allmänna uppgifter

Du kan använda Privacy Manager med följande Microsoft-produkter:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Använda Privacy Manager i Microsoft Outlook

När Privacy Manager är installerat visas knappen Privacy (Sekretess) i Microsoft Outlooks verktygsfält och knappen Send Securely (Skicka säkert) i verktygsfältet i alla e-postmeddelanden i Microsoft Outlook. När du klickar på nedåtpilen vid **Privacy** (Sekretess) eller **Send Securely** (Skicka säkert) kan du välja bland följande alternativ:

- Sign and Send (Send Securely button only) (Signera och skicka (Endast knappen Skicka säkert) – Det här alternativet lägger till en digital signatur i e-postmeddelandet och skickar det när du har autentiserat dig med den valda metoden för säker inloggning.
- Seal for Trusted Contacts and Send (Send Securely button only) (Försegla för betrodda kontakter och skicka (Endast knappen Skicka säkert) – Det här alternativet lägger till en digital signatur, krypterar e-postmeddelandet och skickar det när du har autentiserat dig med den valda metoden för säker inloggning.
- Invite Contacts (Bjud in kontakter) – Med det här alternativet kan du skicka en inbjudan till betrodda kontakter. Mer information finns i Lägga till en betrodd kontakt på sidan 51.
- Invite Outlook Contacts (Bjud in Outlook-kontakter) – Med det här alternativet kan du skicka en inbjudan till betrodda kontakter och ta med alla kontakter i din adressbok i Microsoft Outlook. Mer information finns i Lägga till betrodda kontakter med kontakter från Microsoft Outlook på sidan 52.
- Open the Privacy Manager software (Öppna Privacy Manager-programmet) – Med alternativen för certifikat, betrodda kontakter och inställningar kan du öppna Privacy Manager-programmet för att lägga till, visa eller ändra de nuvarande inställningarna. Mer information finns i Konfigurera Privacy Manager för Microsoft Outlook på sidan 54.

Konfigurera Privacy Manager för Microsoft Outlook

1. Öppna Privacy Manager, klicka på **Settings** (Inställningar) och klicka sedan på fliken **E-mail** (E-post).

   – eller –

   I huvudverktygsfältet i Microsoft Outlook klickar du på nedåtpilen bredvid **Send Securely** (Skicka säkert) (**Privacy** (Sekretess) i Outlook 2003) och sedan på **Settings** (Inställningar).

   – eller –

   I verktygsfältet i ett e-postmeddelande i Microsoft Outlook klickar du på nedåtpilen bredvid **Send Securely** (Skicka säkert) och sedan på **Settings** (Inställningar).

2. Välj vilka åtgärder du vill utföra när du skickar ett säkert e-postmeddelande och klicka på **OK**.

Signera och skicka ett e-postmeddelande

1. I Microsoft Outlook: Klicka på **Nytt** eller **Svara**.
2. Skriv e-postmeddelandet.
3. Klicka på nedåtpilen bredvid **Send Securely** (Skicka säkert) (**Privacy** (Sekretess) i Outlook 2003) och klicka sedan på **Sign and Send** (Signera och skicka).
4. Autentisera dig med önskad metod för säker inloggning.

Försegla och skicka ett e-postmeddelande

Förseglade e-postmeddelanden som är digitalt signerade och förseglade (krypterade) kan bara visas av mottagare du väljer på listan med betrodda kontakter.

Så här förseglar och skickar du ett e-postmeddelande till en betrodd kontakt:

1. I Microsoft Outlook: Klicka på **Nytt** eller **Svara**.
2. Skriv e-postmeddelandet.
3. Klicka på nedåtpilen bredvid **Send Securely** (Skicka säkert) (**Privacy** (Sekretess) i Outlook 2003) och klicka sedan på **Seal for Trusted Contacts and Send** (Försegla åt betrodda kontakter och skicka).
4. Autentisera dig med önskad metod för säker inloggning.

Visa ett förseglat e-postmeddelande

När du öppnar ett förseglat e-postmeddelande visas säkerhetsmärkningen i e-postens rubrik. Säkerhetsmärkningen ger följande information:

- Vilka behörighetskontroller som använts för identifiering av den som signerat e-postmeddelandet
- Vilken produkt som använts för verifiering av behörighetskontrollerna för den som signerat e-postmeddelandet

Använda Privacy Manager i ett Microsoft Office 2007-dokument

OBS! Privacy Manager kan bara användas med Microsoft Office 2007-dokument.

När du har installerat ditt Privacy Manager-certifikat, visas knappen Sign and Encrypt (Signera och kryptera) till höger i verktygsfältet i alla Microsoft Word-, Microsoft Excel- och Microsoft PowerPoint-dokument. När du klickar på nedåtpilen vid **Sign and Encrypt** (Signera och kryptera) kan du välja bland följande alternativ:

- Sign Document (Signera dokument) – Med det här alternativet kan du lägga till en digital signatur i dokumentet.
- Add Signature Line Before Signing (Microsoft Word and Microsoft Excel only) (Lägg till signaturrad före signering (endast Microsoft Word och Microsoft Excel)) – Som standard läggs en signaturrad till när ett Microsoft Word- eller Microsoft Excel-dokument signeras eller krypteras. Du stänger av det här alternativet genom att klicka på **Add Signature Line** (Lägg till signaturrad) så att kryssmarkeringen försvinner.
- Encrypt Document (Kryptera dokument) – Det här alternativet lägger till en digital signatur och krypterar dokumentet.

- Remove Encryption (Ta bort kryptering) – Det här alternativet tar bort krypteringen från dokumentet.
- Open the Privacy Manager software (Öppna Privacy Manager-programmet) – Med alternativen för certifikat, betrodda kontakter och inställningar kan du öppna Privacy Manager-programmet för att lägga till, visa eller ändra de nuvarande inställningarna. Mer information finns i Hantera Privacy Manager-certifikat på sidan 47, Hantera betrodda kontakter på sidan 51 och Konfigurera Privacy Manager för Microsoft Office på sidan 56.

Konfigurera Privacy Manager för Microsoft Office

1. Öppna Privacy Manager, klicka på **Settings** (Inställningar) och klicka sedan på fliken **Documents** (Dokument).

   – eller –

   I verktygsfältet i ett Microsoft Office-dokument klickar du på nedåtpilen bredvid **Sign and Encrypt** (Signera och kryptera) och sedan på **Settings** (Inställningar).

2. Välj vilka åtgärder du vill konfigurera och klicka på **OK**.

Signera ett Microsoft Office-dokument

1. Skapa och spara ett dokument i Microsoft Word, Microsoft Excel eller Microsoft PowerPoint.
2. Klicka på nedåtpilen bredvid **Sign and Encrypt** (Signera och kryptera) och klicka på **Sign Document** (Signera dokument).
3. Autentisera dig med önskad metod för säker inloggning.
4. När dialogrutan för bekräftelse öppnas, ska du läsa texten och sedan klicka på **OK**.

Gör så här om du senare bestämmer dig för att redigera dokumentet:

1. Klicka på knappen **Office** i skärmens övre vänstra hörn.
2. Klicka på **Prepare** (Förbered) och klicka sedan på **Mark as Final** (Markera som slutligt).
3. Klicka på **Yes** (Ja) när dialogrutan för bekräftelse visas och fortsätt ditt arbete.
4. När du är färdig med redigeringen, ska du signera dokumentet igen.

Lägga till en signaturrad vid signering av ett Microsoft Word- eller Microsoft Excel-dokument

Med Privacy Manager kan du lägga till en signaturrad när du signerar ett Microsoft Word- eller Microsoft Excel-dokument:

1. Skapa och spara ett dokument i Microsoft Word eller Microsoft Excel.
2. Klicka på menyn **Home** (Hem).
3. Klicka på nedåtpilen bredvid **Sign and Encrypt** (Signera och kryptera) och klicka på **Add Signature Line Before Signing** (Lägg till signaturrad före signering).

OBS! En bockmarkering visas bredvid Add Signature Line Before Signing (Lägg till signaturrad före signering) när detta alternativ är valt. Alternativet är aktiverat som standard.

4. Klicka på nedåtpilen bredvid **Sign and Encrypt** (Signera och kryptera) och klicka på **Sign Document** (Signera dokument).

5. Autentisera dig med önskad metod för säker inloggning.

Lägga till signatursättare i Microsoft Word- eller Microsoft Excel-dokument

Du kan lägga till mer än en signaturrad i dokumentet genom att utse flera signatursättare. En signatursättare är en användare som är utsedd av ägaren till ett Microsoft Word- eller Microsoft Excel-dokument att lägga till en signaturrad i dokumentet. En signatursättare kan vara du själv eller någon annan som du vill ska signera ditt dokument. Om du exempelvis förbereder ett dokument som måste signeras av all personal på din avdelning, kan du inkludera signaturrader för de användarna längst ned på den sista sidan i dokumentet, med anvisningar för signering ett visst datum.

Så här lägger du till en signatursättare i ett Microsoft Word- eller Microsoft Excel-dokument:

1. Skapa och spara ett dokument i Microsoft Word eller Microsoft Excel.

2. Klicka på menyn **Insert** (Infoga).

3. I gruppen **Text** i verktygsfältet klickar du på pilen bredvid **Signature Line** (Signaturrad) och sedan på **Privacy Manager Signature Provider** (Signatursättare i Privacy Manager).

   Dialogrutan för signaturinställning öppnas.

4. I rutan under **Suggested signer** (Signatursättare) skriver du namnet på signatursättaren.

5. I rutan under **Instructions to the signer** (Anvisningar för signatursättaren) skriver du ett meddelande till den här signatursättaren.

OBS! Meddelandet kommer att visas som en titel, och blir antingen raderat eller ersatt av användarens titel när dokumentet signeras.

6. Markera kryssrutan **Show sign date in signature line** (Visa signeringsdatum på signaturrad) om du vill att datumet ska visas.

7. Markera kryssrutan **Show signer's title in signature line** (Visa signatursättares titel på signaturrad) om du vill att titeln ska visas.

OBS! Ägaren till ett dokument tilldelar sina egna dokument en signatursättare. Därför kommer signatursättaren inte att kunna visa datumet och/eller titeln på signaturraden, även om dennes dokumentinställningar är konfigurerade att göra det, om kryssrutorna **Show sign date in signature line** (Visa signeringsdatum på signaturrad) och/eller **Show signer's title in signature line** (Visa signatursättares titel på signaturrad) inte är markerade.

8. Klicka på **OK**.

Lägga till en signatursättares signaturrad

När en signatursättare öppnar dokumentet ser han eller hon sitt namn inom hakparentes, vilket visar att han/hon måste ange sin signatur.

Så här signeras dokumentet:

1. Dubbelklicka på lämplig signaturrad.

2. Autentisera dig med önskad metod för säker inloggning.

   Signaturraden visas enligt de inställningar som angivits av dokumentets ägare.

Kryptera ett Microsoft Office-dokument

Du kan kryptera ett Microsoft Office-dokument åt dig själv och åt betrodda kontakter. När du kryperar ett dokument och sedan stänger det, måste du och den eller de betrodda kontakter du väljer från listan autentisera er innan dokumentet går att öppna.

Så här krypterar du ett Microsoft Office-dokument:

1. Skapa och spara ett dokument i Microsoft Word, Microsoft Excel eller Microsoft PowerPoint.
2. Klicka på menyn **Home** (Hem).
3. Klicka på nedåtpilen bredvid **Sign and Encrypt** (Signera och kryptera) och klicka sedan på **Encrypt Document** (Kryptera dokument).

   Dialogrutan Select Trusted Contacts (Välj betrodda kontakter) öppnas.
4. Klicka på namnet på en betrodd kontakt som ska kunna öppna dokumentet och se dess innehåll.

OBS! Du kan välja flera betrodda kontakter. Håll ned ctrl-tangenten och klicka på varje namn.

5. Klicka på **OK**.

Följ stegen i Ta bort kryptering från ett Microsoft Office-dokument på sidan 58 om du senare bestämmer dig för att redigera dokumentet. När krypteringen tas bort kan du redigera dokumentet. Utför stegen i det här avsnittet när du vill kryptera dokumentet igen.

Ta bort kryptering från ett Microsoft Office-dokument

När du tar bort krypteringen från ett Microsoft Office-dokument, behöver du och dina betrodda kontakter inte längre autentisera er för att öppna och visa innehållet i dokumentet.

Så här tar du bort kryptering från ett Microsoft Office-dokument:

1. Öppna ett krypterat Microsoft Word-, Microsoft Excel- eller Microsoft PowerPoint-dokument.
2. Autentisera dig med önskad metod för säker inloggning.
3. Klicka på menyn **Home** (Hem).
4. Klicka på nedåtpilen bredvid **Sign and Encrypt** (Signera och kryptera) och klicka sedan på **Remove Encryption** (Ta bort kryptering).

Skicka ett krypterat Microsoft Office-dokument

Du kan bifoga ett krypterat Microsoft Office-dokument i ett e-postmeddelande utan att signera eller kryptera själva e-postmeddelandet. Det här utför du genom att skapa och skicka ett e-postmeddelande med ett signerat eller krypterat dokument, precis som ett vanligt e-postmeddelande med en bilaga.

För bästa möjliga säkerhet bör du dock kryptera e-postmeddelandet när du bifogar ett signerat eller krypterat Microsoft Office-dokument.

Så här skickar du ett förseglat e-postmeddelande med ett bifogat signerat och/eller krypterat Microsoft Office-dokument:

1. I Microsoft Outlook: Klicka på **Nytt** eller **Svara**.
2. Skriv e-postmeddelandet.

3. Bifoga Microsoft Office-dokumentet.

4. Detaljerade instruktioner finns i Försegla och skicka ett e-postmeddelande på sidan 55.

Visa ett signerat Microsoft Office-dokument

OBS! Du behöver inte ha något Privacy Manager-certifikat för att kunna visa ett signerat Microsoft Office-dokument.

När ett signerat Microsoft Office-dokument öppnas, visas en ikon för digital signatur i statusfältet längst ned i dokumentfönstret.

1. Klicka på ikonen **Digital Signatures** (Digitala signaturer) så att visningen växlar till signaturdialogrutan, som visar namnet på alla användare som har signerat dokumentet och det datum som varje användare signerade det.

2. Om du vill visa ytterligare detaljer om varje signatur, högerklickar du på ett namn i dialogrutan för signaturer och väljer Signature Details (Signaturdetaljer).

Visa ett krypterat Microsoft Office-dokument

För att du ska kunna visa ett krypterat Microsoft Office-dokument på en annan dator måste Privacy Manager vara installerat på den datorn. Du måste också återställa det Privacy Manager-certifikat som användes för kryptering av filen.

En betrodd kontakt som vill visa ett krypterat Microsoft Office-dokument måste ha ett Privacy Manager-certifikat och Privacy Manager måste vara installerat på hans eller hennes dator. Den betrodda kontakten måste också vara vald av ägaren till det krypterade Microsoft Office-dokumentet.

Använda Privacy Manager i Windows Live Messenger

Privacy Manager lägger till följande säkerhetsfunktioner för kommunikation i Windows Live Messenger:

- **Secure chat** (Säker chatt) – Meddelanden överförs med SSL/TLS (Secure Sockets Layer/Transport Layer Security) över XML-protokoll, samma teknik som ger säkerhet i e-handelstransaktioner.
- **Recipient identification** (Mottagaridentifiering) – Du kan verifiera en persons identitet och att han eller hon är på plats innan du skickar ett meddelande.
- **Signed messages** (Signerade meddelanden) – Du kan signera dina meddelanden elektroniskt. Om någon sedan mixtrar med meddelandet markeras det som ogiltigt när mottagaren får det.
- **Hide/show** (Dölj/visa) – Du kan dölja ett eller alla meddelanden i Privacy Managers chattfönster. Du kan också skicka ett meddelande där innehållet är dolt. Autentisering krävs innan meddelandet visas.
- **Secure chat history** (Säker chatthistorik) – Loggar över dina chattsessioner krypteras innan de sparas och kräver autentisering för att kunna ses.
- **Automatic locking/unlocking** (Automatisk låsning/upplåsning) – Du kan låsa och låsa upp Privacy Managers chattfönster eller ställa in det på att låsas automatiskt efter en viss period av inaktivitet.

Starta chattsession i Privacy Manager

OBS! För att man ska kunna använda Privacy Manager Chat måste båda parter ha Privacy Manager och ett Privacy Manager-certifikat installerat. Mer information om hur du installerar ett Privacy Manager-certifikat finns i Beställa och installera ett Privacy Manager-certifikat på sidan 47.

1. Starta Privacy Manager Chat i Windows Live Messenger enligt någon av följande procedurer:

   a. Högerklicka på en online-kontakt i Live Messenger och välj sedan **Starta en aktivitet**.

   b. Klicka på **Start Chat** (Starta chatt).

   – eller –

   a. Dubbelklicka på en online-kontakt i Live Messenger och välj sedan menyn **See a list of activities** (Visa lista med aktiviteter).

   b. Klicka på **Action** (Åtgärd) och sedan på **Start Chat** (Starta chatt).

   – eller –

   a. Högerklicka på **ProtectTools**-ikonen i meddelandefältet, klicka på **Privacy Manager for HP ProtectTools** (Privacy Manager för HP ProtectTools) och välj sedan **Start Chat** (Starta chatt).

   b. I Live Messenger klickar du på **Actions: Start an Activity** (Åtgärder: Starta en aktivitet) och välj sedan **Privacy Manager Chat** (Privacy Manager-chatt).

   OBS! Varje användare måste vara online i Live Messenger och användarna måste visas i varandras online-fönster i Live Messenger. Klicka och välj en användare som är online.

   Privacy Manager skickar en inbjudan till kontakten om att börja chatta i Privacy Manager Chat. När den inbjudna kontakten tackat ja, öppnas fönstret Privacy Manager Chat. Om den inbjudna kontakten inte har Privacy Manager, blir han eller hon uppmanad att ladda ned det.

2. Klicka på **Start** och påbörja den säkra chattsessionen.

Konfigurera Privacy Manager för Windows Live Messenger

1. I Privacy Manager Chat: Klicka på knappen **Settings** (Inställningar).

   – eller –

   I Privacy Manager: Klicka på **Settings** (Inställningar) och klicka sedan på fliken **Chat** (Chatta).

   – eller –

   I Privacy Manager Live Messenger History Viewer: Klicka på knappen **Settings** (Inställningar).

2. Ange hur länge Privacy Manager Chat ska vänta innan det låser sessionen: Välj ett tal i listan **Lock session after _ minutes of activity** (Lås session efter _ minuters aktivitet).

3. Ange en historikmapp för dina chattsessioner: Klicka på **Browse** (Bläddra) och sök efter en mapp. Klicka sedan på **OK**.

4. Om du vill att dina sessioner ska krypteras och sparas automatiskt när du stänger dem, markerar du kryssrutan **Automatically save secure chat history** (Spara automatiskt säker chatthistorik).

5. Klicka på **OK**.

Chatta i Privacy Manager Chat-fönstret

När du har startat Privacy Manager Chat, öppnas ett Privacy Manager Chat-fönster i Windows Live Messenger. Privacy Manager Chat används ungefär som den klassiska versionen av Windows Live Messenger, förutom att följande extrafunktioner finns i Privacy Manager Chat-fönstret:

- **Save** (Spara) – Klicka på den här knappen när du vill spara chattsessionen i den mapp som är angiven i konfigurationsinställningarna. Du kan också konfigurera Privacy Manager Chat så att det automatiskt sparar varje session när det stängs.
- **Hide all** (Dölj alla) och **Show all** (Visa alla) – Klicka på önskad knapp när du vill dölja respektive visa meddelanden i fönstret Secure Communications (Säker kommunikation). Du kan också dölja eller visa separata meddelanden genom att klicka i deras meddelanderubrik.
- **Are you there?** (Är du där?) – Klicka på den här knappen när du vill ha en bekräftelse från en kontakt.
- **Lock** (Lås) – Klicka på den här knappen när du vill stänga fönstret Privacy Manager Chat och gå tillbaka till chattfönstret. Du kan visa fönstret Secure Communications (Säker kommunikation) igen genom att klicka på **Resume the session** (Fortsätt sessionen) och sedan autentisera dig med önskad metod för säker inloggning.
- **Send** (Skicka) – Klicka på den här knappen om du vill skicka ett krypterat meddelande till en kontakt.
- **Send signed** (Skicka signerat) – Markera den här kryssrutan om du vill signera dina meddelanden elektroniskt och kryptera dem. Om någon sedan mixtrar med meddelandet markeras det som ogiltigt när mottagaren får det. Du måste autentisera dig varje gång du skickar ett signerat meddelande.
- **Send hidden** (Skicka dolt) – Markera den här kryssrutan när du vill kryptera och skicka ett meddelande där bara rubriken visas. Din kontakt måste då autentisera sig för att kunna läsa meddelandet.

Visa chatthistorik

Privacy Manager Chat: Live Messenger History Viewer visar krypterade sessionsfiler i Privacy Manager Chat. Du kan spara sessionerna genom att klicka på **Save** (Spara) i Privacy Manager Chat-fönstret, eller ställa in den automatiska sparfunktionen på fliken Chat (Chatt) i Privacy Manager. I Viewer visar varje session kontaktens namn (krypterat) på skärmen och datum och tid för sessionens början och slut. Som förinställning visas sessionerna för alla e-postkonton du har ställt in. Du kan använda menyn **Display history for** (Visa historik för) om du vill att enbart vissa konton ska visas.

I Viewer kan du utföra följande aktiviteter:

- Visa alla sessioner på sidan 62
- Visa sessioner för ett visst konto på sidan 62
- Visa ett sessions-ID på sidan 62
- Visa en session på sidan 63
- Sök efter sessioner med specifik text på sidan 63
- Radera en session på sidan 63

- Lägga till eller ta bort kolumner på sidan 63
- Filtrera visade sessioner på sidan 64

Så här startar du Live Messenger History Viewer:

▲ Högerklicka på ikonen **HP ProtectTools** i meddelandefältet längst till höger i Aktivitetsfältet, klicka på **Privacy Manager: for HP ProtectTools** (Privacy Manager för HP ProtectTools) och klicka sedan på **Live Messenger History Viewer**.

– eller –

▲ I en chattsession: Klicka på **History Viewer** (Historikvisning) eller **History** (Historik).

Visa alla sessioner

När du visar alla sessioner visas kontaktens dekrypterade namn på skärmen för den eller de valda sessionerna och alla sessioner inom samma konto.

Så här visar du alla dina sparade chatthistoriksessioner:

1. I Live Messenger History Viewer: Högerklicka på valfri session och välj **Reveal All Sessions** (Visa alla sessioner).
2. Autentisera dig med önskad metod för säker inloggning.

   Kontakternas namn visas dekrypterade.
3. Dubbelklicka på valfri session när du vill se innehållet.

Visa sessioner för ett visst konto

När du visar en session visas kontaktens dekrypterade namn på skärmen för den valda sessionen.

Så här visar du en specifik chatthistoriksession:

1. I Live Messenger History Viewer: Högerklicka på valfri session och välj **Reveal Session** (Visa session).
2. Autentisera dig med önskad metod för säker inloggning.

   Kontaktens namn visas dekrypterat.
3. Dubbelklicka på den visade sessionen när du vill se innehållet.

OBS! Övriga sessioner som är krypterade med samma certifikat visar en upplåst ikon, vilket indikerar att du kan visa de sessionerna genom att dubbelklicka på någon av dem utan ytterligare autentisering. Sessioner som är krypterade med ett annat certifikat visar en låst ikon, vilket indikerar att ytterligare autentisering krävs för de sessionerna innan du kan visa kontakternas namn på skärmen eller sessionernas innehåll.

Visa ett sessions-ID

Så här visar du ett sessions-ID:

▲ I Live Messenger History Viewer: Högerklicka på en visad session och välj **View session ID** (Visa sessions-ID).

Visa en session

När du visar en session öppnas filen för visning. Om sessionen inte har visats tidigare (och kontaktens namn visas dekrypterat på skärmen), visas den samtidigt.

Så här visar du en historiksession i Live Messenger:

1. I Live Messenger History Viewer: Högerklicka på valfri session och välj **View** (Visa).
2. Autentisera dig med önskad metod för säker inloggning om du uppmanas göra det.

   Sessionens innehåll dekrypteras.

Sök efter sessioner med specifik text

Du kan bara söka efter text i visade (dekrypterade) sessioner som visas i Viewer-fönstret. Detta är de sessioner vars kontaktnamn visas på skärmen med vanlig text.

Så här söker du efter text i chatthistoriksessioner:

1. I Live Messenger History Viewer: Klicka på knappen **Search** (Sök).
2. Ange söktexten, ställ in eventuella sökparametrar och klicka på **OK**.

   Sessioner som innehåller texten markeras i Viewer-fönstret.

Radera en session

1. Välj en chatthistoriksession.
2. Klicka på **Delete** (Radera).

Lägga till eller ta bort kolumner

Som standard visas de 3 mest använda kolumnerna i Live Messenger History Viewer. Du kan lägga till ytterligare kolumner på skärmen, eller ta bort kolumner från skärmen.

Så här lägger du till kolumner på skärmen:

1. Högerklicka på en kolumnrubrik och välj **Add/Remove Columns** (Lägg till/ta bort kolumner).
2. Markera en kolumnrubrik i vänster panel och klicka sedan på **Add** (Lägg till) så att den flyttas till höger panel.

Så tar du bort kolumner från skärmen:

1. Högerklicka på en kolumnrubrik och välj **Add/Remove Columns** (Lägg till/ta bort kolumner).
2. Markera en kolumnrubrik i höger panel och klicka sedan på **Remove** (Ta bort) så att den flyttas till vänster panel.

Filtrera visade sessioner

En lista med sessioner för alla dina konton visas i Live Messenger History Viewer. Du kan också filtrera visade sessioner för följande:

- Specifika konton. Mer information finns i Visa sessioner för ett visst konto på sidan 64.
- Datumintervall. Mer information finns i Visa sessioner för ett datumintervall på sidan 64.
- Olika mappar. Mer information finns i Visa sessioner som sparats i en annan mapp än standardmappen på sidan 64.

Visa sessioner för ett visst konto

▲ I Live Messenger History Viewer: Välj ett konto på menyn **Display history for** (Visa historik för).

Visa sessioner för ett datumintervall

1. I Live Messenger History Viewer: Klicka på knappen **Advanced Filter** (Avancerat filter).

   Dialogrutan för avancerat filter öppnas.

2. Markera kryssrutan **Display only sessions within specified date range** (Visa endast sessioner inom angivet datumintervall).
3. I rutorna **From date** (Från-datum) och **To date** (Till-datum) anger du dag, månad och/eller år, eller väljer datum genom att klicka på pilen vid kalendern.
4. Klicka på **OK**.

Visa sessioner som sparats i en annan mapp än standardmappen

1. I Live Messenger History Viewer: Klicka på knappen **Advanced Filter** (Avancerat filter).
2. Markera kryssrutan **Use an alternate history files folder** (Använd annan mapp för historikfiler).
3. Ange mappens sökväg eller klicka på **Browse** (Bläddra) och sök efter en mapp.
4. Klicka på **OK**.

Avancerade uppgifter

Migrera Privacy Manager-certifikat och betrodda kontakter till en annan dator

Du kan på ett säkert sätt migrera dina Privacy Manager-certifikat och betrodda kontakter till en annan dator, eller säkerhetskopiera data för förvaring. Det gör du genom att säkerhetskopiera dina data som en lösenordsskyddad fil till en plats i nätverket eller en flyttbar lagringsenhet och sedan återställa filen på den nya datorn.

Säkerhetskopiera Privacy Manager-certifikat och betrodda kontakter

Så här säkerhetskopierar du Privacy Manager-certifikat och betrodda kontakter till en lösenordsskyddad fil:

1. Öppna Privacy Manager och klicka på **Migration** (Migrering).
2. Klicka på **Backup** (Säkerhetskopiera).
3. På sidan Select Data (Välj data) väljer du vilka datakategorier som ska inkluderas i migrationsfilen och klickar sedan på **Next** (Nästa).
4. På sidan Migration File (Migrationsfil) anger du ett filnamn eller klickar på **Browse** (Bläddra) så att du kan söka efter en plats. Klicka sedan på **Next** (Nästa).
5. Ange och bekräfta ett lösenord och klicka sedan på **Next** (Nästa).

OBS! Förvara detta lösenord på en säker plats. Du kommer att behöva det när du återställer migrationsfilen.

6. Autentisera dig med önskad metod för säker inloggning.
7. På sidan Migration File Saved (Migrationsfil sparad) klickar du på **Finish** (Slutför).

Återställa Privacy Manager-certifikat och betrodda kontakter

Så här återställer du dina Privacy Manager-certifikat och betrodda kontakter på en annan dator som en del av migrationsprocessen eller till samma dator:

1. Öppna Privacy Manager och klicka på **Migration** (Migrering).
2. Klicka på **Restore** (Återställ).
3. På sidan Migration File (Migrationsfil) klickar du på **Browse** (Bläddra) så att du kan söka efter filen. Klicka sedan på **Next** (Nästa).
4. Ange det lösenord du använde när du skapade filen med säkerhetskopian och klicka sedan på **Next** (Nästa).
5. På sidan Migration File (Migrationsfil) klickar du på **Finish** (Slutför).

Central administration av Privacy Manager

Din installation av Privacy Manager kan vara en del av en centraliserad installation, som har specialinställts av din administratör. En eller flera av följande funktioner kan antingen vara aktiverad eller inaktiverad:

- **Certificate use policy** (Princip för certifikatanvändning) – Det kan hända att du bara får använda Privacy Manager-certifikat som är utfärdade av Comodo, eller också får du använda digitala certifikat som utfärdats av andra certifierande myndigheter.
- **Encryption policy** (Krypteringsprincip) – Krypteringsfunktionerna kan vara aktiverade eller inaktiverade en och en i Microsoft Office eller Outlook och i Windows Live Messenger.

10 File Sanitizer for HP ProtectTools

Med File Sanitizer kan du på ett säkert sätt "strimla" (shred) digitala objekt (personlig information eller filer, historik- eller webbrelaterat innehåll eller andra datakomponenter) i datorn och regelbundet använda funktionen bleaching på hårddisken.

OBS! Den här versionen av File Sanitizer kan du bara använda på systemets hårddisk.

Shredding

Shredding fungerar annorlunda än en vanlig radering i Windows® (även kallad simple delete (enkel radering) i File Sanitizer). När du använder shredding med File Sanitizer på ett objekt anropas en algoritm som döljer informationen i objektet, vilket gör det i stort sett omöjligt att återskapa det ursprungliga objektet. En simple delete (enkel radering) i Windows kan lämna kvar filen (eller objektet) intakt på hårddisken eller i ett tillstånd där kriminaltekniska metoder skulle kunna användas för att återställa filen (eller objektet).

När du väljer en shredding-profil (med hög, medelhög eller låg säkerhet), väljs en fördefinierad lista med objekt och en raderingsmetod automatiskt för shredding-processen. Du kan också anpassa en shredding-profil och ange hur många shredding-cykler som ska utföras, på vilka objekt shredding ska användas, vilka objekt som ska bekräftas innan shredding används och på vilka objekt shredding inte ska användas. Mer information finns i Välja eller skapa en shredding-profil på sidan 71.

Du kan ställa in ett automatiskt shredding-schema, men också använda shredding manuellt på objekt när du vill. Mer information finns i Skapa ett shredding-schema på sidan 70, Manuell shredding på ett objekt på sidan 75 och Manuell shredding på alla markerade objekt på sidan 75.

OBS! En .dll-fil kan endast raderas med shredding och tas bort från systemet om den först har flyttats till papperskorgen.

Free space bleaching

När du raderar ett objekt i Windows försvinner inte objektets innehåll helt och hållet från hårddisken. Windows raderar bara referensen till objektet. Innehållet ligger fortfarande kvar på hårddisken tills ett annat objekt skriver över samma område på hårddisken med ny information.

Free space bleaching är en säker metod som skriver över objekt med slumpmässigt valda data, vilket gör att det inte går att visa det ursprungliga innehållet i det raderade objektet.

OBS! Free space bleaching är avsett för objekt du raderar med Windows papperskorg eller raderar manuellt. Free space bleaching ger ingen ytterligare säkerhet för objekt som du använt shredding på.

Du kan ställa in ett automatiskt schema för free space bleaching eller manuellt aktivera free space bleaching med ikonen **HP ProtectTools** i meddelandefältet längst till höger i Aktivitetsfältet. Mer information finns i Skapa ett schema för free space bleaching på sidan 71 och Manuell aktivering av free space bleaching på sidan 76.

Installation

Öppna File Sanitizer

Så här öppnar du File Sanitizer:

1. Klicka på **Start**, **Alla program**, **HP** och **HP ProtectTools Security Manager**.
2. Klicka på **File Sanitizer**.

– eller –

▲ Dubbelklicka på ikonen **File Sanitizer** på skrivbordet.

– eller –

▲ Högerklicka på ikonen **HP ProtectTools** i meddelandefältet längst till höger i Aktivitetsfältet, klicka på **File Sanitizer** och klicka sedan på **Open File Sanitizer** (Öppna File Sanitizer).

Skapa ett shredding-schema

OBS! Information om hur du väljer en fördefinierad shredding-profil eller skapar en shredding-profil finns i Välja eller skapa en shredding-profil på sidan 71.

OBS! Mer information om hur man använder manuell shredding på objekt finns i Manuell shredding på ett objekt på sidan 75.

1. Öppna File Sanitizer och klicka på **Shred** (Använd shredding).
2. Välj ett shredding-alternativ:
   - **Windows shutdown** (Avstängning av Windows) – Välj detta alternativ om du vill att shredding ska användas på alla valda objekt när Windows stängs av.

     OBS! När detta alternativ är valt, visas en dialogruta vid avstängning som frågar om du vill fortsätta att använda shredding på de valda objekten eller vill att proceduren ska ignoreras. Klicka på **Yes** (Ja) om du vill att shredding-proceduren ska ignoreras. Klicka på **No** (Nej) om du vill fortsätta att använda shredding.

   - **Web browser open** (Start av webbläsare) – Välj det här alternativet om du vill att shredding ska användas på alla valda webbrelaterade objekt, t.ex. webbläsarens URL-historik, när du öppnar en webbläsare.
   - **Web browser quit** (Stängning av webbläsare) – Välj det här alternativet om du vill att shredding ska användas på alla valda webbrelaterade objekt, t.ex. webbläsarens URL-historik, när du stänger en webbläsare.
   - **Key sequence** (Tangentsekvens) – Välj det här alternativet när du vill initiera shredding med en tangentsekvens.
   - **Scheduler** (Schemaläggning) – Markera kryssrutan **Activate Scheduler** (Aktivera schemaläggning), ange ditt Windows-lösenord och ange datum och tid när shredding ska användas på valda objekt.

   OBS! En .dll-fil kan endast raderas med shredding och tas bort från systemet om den först har flyttats till papperskorgen.
3. Klicka på **Apply** (Verkställ) och sedan på **OK**.

Skapa ett schema för free space bleaching

OBS! Free space bleaching är avsett för objekt du raderar med Windows papperskorg eller raderar manuellt. Free space bleaching ger ingen ytterligare säkerhet för objekt som du använt shredding på.

Så här skapar du ett schema för free space bleaching:

1. Öppna File Sanitizer och klicka på **Free Space Bleaching**.
2. Markera kryssrutan **Activate Scheduler** (Aktivera schemaläggning), ange ditt Windows-lösenord och ange datum och tid då free space bleaching ska utföras på hårddisken.
3. Klicka på **Apply** (Verkställ) och sedan på **OK**.

OBS! En procedur med free space bleaching kan ta lång tid. Trots att free space bleaching utförs i bakgrunden, kan datorn arbeta långsammare beroende på den ökade processoranvändningen.

Välja eller skapa en shredding-profil

Du kan ange en raderingsmetod och välja vilka objekt som shredding ska användas på genom att välja en fördefinierad profil eller skapa en egen.

Välja en fördefinierad shredding-profil

När du väljer en fördefinierad shredding-profil (med hög, medelhög eller låg säkerhet), väljs en fördefinierad raderingsmetod och lista över objekt automatiskt. Klicka på knappen **View Details** (Visa detaljer) om du vill se den fördefinierade listan med objekt som har valts för shredding.

Så här väljer du en fördefinierad shredding-profil:

1. Öppna File Sanitizer och klicka på **Settings** (Inställningar).
2. Klicka på en fördefinierad shredding-profil.
3. Klicka på **View Details** (Visa detaljer) om du vill se listan med objekt som är valda för shredding.
4. Under **Shred the following** (Använd shredding på följande) markerar du kryssrutan bredvid varje objekt du vill bekräfta innan shredding körs.
5. Klicka på **Apply** (Verkställ) och sedan på **OK**.

Anpassa en shredding-profil

När du skapar en shredding-profil anger du hur många shredding-cykler som ska köras, på vilka objekt shredding ska användas, vilka objekt som ska bekräftas innan shredding används och på vilka objekt shredding inte ska användas:

1. Öppna File Sanitizer och klicka på **Settings** (Inställningar), klicka på **Advanced Security Settings** (Avancerade säkerhetsinställningar) och klicka sedan på **View Details** (Visa detaljer).
2. Ange antalet shredding-cykler.

OBS! Det valda antalet shredding-cykler kommer att utföras på varje objekt. Om du t.ex. väljer 3 shredding-cykler, exkeveras en algoritm som döljer data i objektet 3 separata gånger. Om du väljer shredding-cykler med högre säkerhet kan proceduren ta ganska lång tid, men ju fler cykler du anger, desto mindre troligt är det att data kan återställas.

3. Välj vilka objekt du vill använda shredding på:

   a. Under **Available shred options** (Tillgängliga shredding-alternativ) klickar du på ett objekt och sedan på **Add** (Lägg till).

   b. Du lägger till ett eget objekt genom att klicka på **Add Custom Option** (Lägg till eget objekt) och sedan bläddra fram eller skriva sökvägen till filnamnet eller mappen. Klicka på **Open** (Öppna) och sedan på **OK**. Under **Available Shred Options** (Tillgängliga shredding-alternativ) klickar du på det egna objektet och sedan på **Add** (Lägg till).

OBS! Du tar bort ett objekt från de tillgängliga shredding-alternativen genom att klicka på objektet och sedan klicka på **Delete** (Radera).

4. Under **Shred the following** (Använd shredding på följande) markerar du kryssrutan bredvid varje objekt du vill bekräfta innan shredding körs.

OBS! Du raderar ett objekt från shredding-listan genom att klicka på objektet och sedan klicka på **Remove** (Ta bort).

5. Så här skyddar du filer eller mappar mot automatisk shredding: Under **Do not shred the following** (Använd inte shredding på följande) klickar du på **Add** (Lägg till) och bläddrar sedan till eller skriver sökvägen till filnamnet eller mappen. Klicka på **Open** (Öppna) och sedan på **OK**.

OBS! Du tar bort ett objekt från listan med uteslutna objekt genom att klicka på objektet och sedan klicka på **Delete** (Radera).

6. När du har konfigurerat shredding-profilen, klickar du på **Apply** (Verkställ) och sedan på **OK**.

Anpassa en profil för simple delete (enkel radering)

Profilen för simple delete utför en vanlig radering av ett objekt utan att använda shredding. När du anpassar en profil för simple delete, anger du vilka objekt som ska inkluderas i raderingen, vilka objekt som ska bekräftas innan raderingen utförs och vilka objekt som ska uteslutas från raderingen.

OBS! Om du använder alternativet för enkel radering (simple delete), kan du utföra free space bleaching emellanåt på objekt som har raderats manuellt eller med Windows papperskorg.

Så här anpassar du en profil för simple delete (enkel radering):

1. Öppna File Sanitizer, klicka på **Settings** (Inställningar), klicka på **Simple Delete Setting** (Inställning för enkel radering) och klicka sedan på **View Details** (Visa detaljer).

2. Välj vilka objekt du vill radera:

   a. Under **Available delete options** (Tillgängliga raderingsalternativ) klickar du på ett objekt och sedan på **Add** (Lägg till).

   b. Du lägger till ett eget objekt genom att klicka på **Add Custom Option** (Lägg till eget alternativ), ange ett fil- eller mappnamn och sedan klicka på **OK**. Klicka på det egna objektet och klicka sedan på **Add** (Lägg till).

OBS! Du raderar ett objekt från de tillgängliga raderingsalternativen genom att klicka på objektet och sedan klicka på **Delete** (Radera).

3. Under **Delete the following** (Radera följande) markerar du kryssrutan bredvid varje objekt du vill bekräfta före radering.

OBS! Du tar bort ett objekt från raderingslistan genom att klicka på objektet och sedan klicka på **Remove** (Ta bort).

4. Under **Do not delete the following** (Radera inte följande) klickar du på **Add** (Lägg till) och väljer de specifika objekt som inte ska raderas.

OBS! Du tar bort ett objekt från listan med uteslutna objekt genom att klicka på objektet och sedan klicka på **Delete** (Radera).

5. När du har konfigurerat profilen för simple delete, klickar du på **Apply** (Verkställ) och sedan på **OK**.

Allmänna uppgifter

Du kan använda File Sanitizer för att utföra följande aktiviteter:

- Use a key sequence to initiate shredding (Initiera shredding med tangentsekvens) – Med den här funktionen skapar du en tangentsekvens (t.ex. ctrl+alt+s) som initierar shredding. Mer information finns i Använda en tangentsekvens för att initiera shredding på sidan 74.
- Use the File Sanitizer icon to initiate shredding (Initiera shredding med File Sanitizer-ikonen) – Den här funktionen liknar dra-och-släpp-funktionen i Windows. Mer information finns i Använda ikonen File Sanitizer på sidan 75.
- Manually shred a specific asset or all selected assets (Utför manuell shredding på ett specifikt objekt eller alla markerade objekt) – De här funktionerna gör att du kan utföra manuell shredding på objekt utan att vänta på att det regelrätta shredding-schemat ska anropas. Mer information finns i Manuell shredding på ett objekt på sidan 75 och Manuell shredding på alla markerade objekt på sidan 75.
- Manually activate free space bleaching (Aktivera free space bleaching manuellt) – Med den här funktionen kan du aktivera free space bleaching manuellt. Mer information finns i Manuell aktivering av free space bleaching på sidan 76.
- Abort a shred or free space bleaching operation (Avbryt shredding eller free space bleaching) – Den här funktionen gör att du kan stoppa en shredding eller free space bleaching som du startat. Mer information finns i Avbryta shredding eller free space bleaching på sidan 76.
- View the log files (Visa loggfilerna) – Med den här funktionen kan du visa loggfiler för shredding och free space bleaching. De innehåller eventuella fel från din senaste shredding eller free space bleaching. Mer information finns i Visa loggfilerna på sidan 76.

OBS! En shredding eller free space bleaching kan ta lång tid att genomföra. Trots att shredding och free space bleaching utförs i bakgrunden, kan datorn arbeta långsammare beroende på den ökade processoranvändningen.

Använda en tangentsekvens för att initiera shredding

Så här anger du en tangentsekvens:

1. Öppna File Sanitizer och klicka på **Shred** (Använd shredding).
2. Markera kryssrutan **Key sequence** (Tangentsekvens).
3. Ange ett tecken i textrutan.
4. Markera antingen kryssrutan **CTRL** eller **ALT** och sedan rutan **SHIFT**.

   Om du t.ex. vill initiera automatisk shredding med s-tangenten och ctrl+shift, anger du tecknet `s` i textrutan och markerar sedan kryssrutorna **CTRL** och **SHIFT**.

OBS! Tänk på att välja en unik tangentsekvens, inte någon tangentsekvens du redan har konfigurerat för något annat.

Så här initierar du shredding med en tangentsekvens:

1. Håll ned shift- och ctrl-tangenten eller alt-tangenten (eller någon annan kombination du har angivit) samtidigt som du trycker på det valda tecknet.
2. Klicka på **Yes** (Ja) om en dialogruta för bekräftelse visas.

Använda ikonen File Sanitizer

△ **VIKTIGT:** Objekt som du använt shredding på kan inte återställas. Tänk noga efter vilka objekt du väljer för manuell shredding.

1. Navigera till dokumentet eller mappen du vill använda shredding på.
2. Dra objektet till ikonen **File Sanitizer** på skrivbordet.
3. Klicka på **Yes** (Ja) när dialogrutan för bekräftelse visas.

Manuell shredding på ett objekt

△ **VIKTIGT:** Objekt som du använt shredding på kan inte återställas. Tänk noga efter vilka objekt du väljer för manuell shredding.

1. Högerklicka på ikonen **HP ProtectTools** i meddelandefältet längst till höger i Aktivitetsfältet, klicka på **File Sanitizer** (Filsanering) och klicka sedan på **Shred One** (Använd shredding på ett).
2. När dialogrutan Browse (Bläddra) öppnas, navigerar du till objektet du vill använda shredding på och klickar sedan på **OK**.

OBS! Det objekt du väljer kan vara en enskild fil eller mapp.

3. Klicka på **Yes** (Ja) när dialogrutan för bekräftelse visas.

– eller –

1. Högerklicka på ikonen **File Sanitizer** på skrivbordet och och klicka sedan på **Shred One** (Använd shredding på ett).
2. När dialogrutan Browse (Bläddra) öppnas, navigerar du till objektet du vill använda shredding på och klickar sedan på **OK**.
3. Klicka på **Yes** (Ja) när dialogrutan för bekräftelse visas.

– eller –

1. Öppna File Sanitizer och klicka på **Shred** (Använd shredding).
2. Klicka på knappen **Browse** (Bläddra).
3. När dialogrutan Browse (Bläddra) öppnas, navigerar du till objektet du vill använda shredding på och klickar sedan på **OK**.
4. Klicka på **Yes** (Ja) när dialogrutan för bekräftelse visas.

Manuell shredding på alla markerade objekt

1. Högerklicka på ikonen **HP ProtectTools** i meddelandefältet längst till höger i Aktivitetsfältet, klicka på **File Sanitizer** och klicka sedan på **Shred Now** (Använd shredding nu).
2. Klicka på **Yes** (Ja) när dialogrutan för bekräftelse visas.

– eller –

1. Högerklicka på ikonen **File Sanitizer** på skrivbordet och och klicka sedan på **Shred Now** (Använd shredding nu).
2. Klicka på **Yes** (Ja) när dialogrutan för bekräftelse visas.

– eller –

1. Öppna File Sanitizer och klicka på **Shred** (Använd shredding).
2. Klicka på knappen **Shred Now** (Använd shredding nu).
3. Klicka på **Yes** (Ja) när dialogrutan för bekräftelse visas.

Manuell aktivering av free space bleaching

1. Högerklicka på ikonen **HP ProtectTools** i meddelandefältet längst till höger i Aktivitetsfältet, klicka på **File Sanitizer** och klicka sedan på **Bleach Now** (Använd bleaching nu).
2. Klicka på **Yes** (Ja) när dialogrutan för bekräftelse visas.

– eller –

1. Öppna File Sanitizer och klicka på **Free Space Bleaching**.
2. Klicka på **Bleach Now** (Använd bleaching nu).
3. Klicka på **Yes** (Ja) när dialogrutan för bekräftelse visas.

Avbryta shredding eller free space bleaching

När shredding eller free space bleaching pågår, visas ett meddelande ovanför ikonen HP ProtectTools Security Manager i meddelandefältet. Meddelandet innehåller uppgifter om shredding- eller free space bleaching-processen (hur mycket som är slutfört i procent) och ger dig möjlighet att avbryta processen.

Så här avbryter du processen:

▲ Klicka på meddelandet och klicka sedan på **Stop** (Stoppa) så att processen avbryts.

Visa loggfilerna

Varje gång shredding eller free space bleaching utförs, genereras loggfiler med eventuella fel. Loggfilerna uppdateras alltid med information om den senaste shredding- eller free space bleaching-processen.

OBS! Filer som har bearbetats med shredding eller bleaching utan problem visas inte i loggfilerna.

En loggfil skapas för shredding och en annan för free space bleaching. Båda loggfilerna ligger på hårddisken:

- C:\Program Files\Hewlett-Packard\File Sanitizer*[Användarnamn]*_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer*[Användarnamn]*_DiskBleachLog.txt

11 Device Access Manager for HP ProtectTools (endast vissa modeller)

Administratörer av operativsystemet Windows® använder Device Access Manager för HP ProtectTools för att styra åtkomsten till enheterna i ett system och skydda mot obehörig åtkomst:

- Enhetsprofiler skapas för varje användare för att definiera vilka enheter som de ska ha åtkomst till.
- Användare är också organiserade i grupper, t ex den fördefinierade Enhetsadministratörer. Grupper kan också vara definerade med alternativet Datorhantering i avsnittet Administrativa verktyg i Kontrollpanelen.
- Enhetsåtkomst kan ges eller nekas baserat på grupptillhörighet.
- För enhetsklasser som CD-ROM-enheter och DVD-enheter kan läs- och skrivåtkomst tillåtas eller nekas separat.

Vissa användare kan också få tillstånd att läsa och modifiera principen för kontroll av enhetsåtkomst.

Installationsprocedurer

Öppna Device Access Manager

Så här öppnar du Device Access Manager:

1. Klicka på **Start**, **Alla program**, **HP** och **HP ProtectTools Administrative Console**.
2. Klicka på **Device Access Manager** (Hanteraren för enhetsåtkomst) i den vänstra rutan.

Konfigurera enhetsåtkomst

Device Access Manager för HP ProtectTools har tre vyer:

- Vyn Simple Configuration (Enkel konfiguration) använder man för att tillåta eller neka åtkomst till klasser med enheter för medlemmarna i gruppen Enhetsadministratörer.
- Vyn Device Class Configuration (Enhetsklasskonfiguration) använder man för att tillåta eller neka åtkomst till typer av enheter eller specifika enheter för specifika användare eller grupper.
- Vyn User Access Settings (Inställningar för användaråtkomst) använder man för att specificera vilka användare som ska kunna se eller modifiera information i Simple Configuration (Enkel konfiguration) och Device Class Configuration (Enhetsklasskonfiguration).

Gruppen Enhetsadministratörer

När Device Access Manager installeras, skapas gruppen Enhetsadministratörer.

Systemadministratören kan implementera en enkel princip för kontroll av enhetsåtkomst genom att neka åtkomst till en uppsättning enhetsklasser, såvida inte en användare klassificeras som betrodd (avseende enhetsåtkomst). Det rekommenderade sättet att skilja mellan "enhetsbetrodda" användare och "icke enhetsbetrodda" användare är att göra alla "enhetsbetrodda användare medlemmar i gruppen Enhetsadministratörer. Att ge medlemmar i gruppen Enhetsadministratörer åtkomst till enheter via vyn Simple Configuration (Enkel konfiguration) eller Device Class Configuration (Enhetsklasskonfiguration) säkerställer därför att "enhetsbetrodda" användare har full åtkomst till den specificerade uppsättningen enhetsklasser.

OBS! Att lägga till en användare i gruppen Enhetsadministratörer ger inte automatiskt den användaren åtkomst till enheter. Vyn Simple Configuration (Enkel konfiguration) kan man dock använda för att ge åtkomst till den erforderliga uppsättningen enhetsklasser för "enhetsbetrodda" användare.

Så här lägger du till användare i gruppen Enhetsadministratörer:

- För Windows 7, Vista eller XP Professional: Använd den vanliga MMC-snapin-modulen "Lokala användare och grupper".
- För hemmaversioner av Windows 7, Vista® eller XP: Från ett privilegierat konto skriver du följande i ett kommandotolksfönster:

```
c:\> net localgroup "Device Administrators" username /ADD
```

Enkel konfiguration

Administratörer och auktoriserade användare kan använda vyn Simple Configuration (Enkel konfiguration) för att modifiera åtkomsten till följande klasser av enheter för alla som inte är enhetsadministratörer:

OBS! För att användaren eller gruppen ska kunna använda den här vyn för att läsa information om enhetsåtkomst, måste användaren eller gruppen ges "läsåtkomst" i vyn **User Access Settings** (Inställningar för användaråtkomst). För att användaren eller gruppen ska kunna visa eller modifiera information om enhetsåtkomst, måste användaren eller gruppen ges "ändringsåtkomst" i vyn **User Access Settings** (Inställningar för användaråtkomst).

- Alla uttagbara medier (disketter, USB-minnen osv.)
- Alla DVD/CD-ROM-enheter
- Alla seriella portar och parallellportar
- Alla Bluetooth®-enheter
- Alla infraröda enheter
- Alla modemenheter
- Alla PCMCIA-enheter
- Alla 1394-enheter

Så här tillåter eller nekar du åtkomst till en klass av enheter för alla som inte är enhetsadministratörer:

1. Klicka på **Device Access Manager** i den vänstra rutan i **HP ProtectTools Administrative Console** och klicka sedan på **Simple Configuration** (Enkel konfiguration).
2. I höger ruta ska du sedan för att neka till åtkomst markera kryssrutan för en enhetsklass eller specifik enhet. Avmarkera kryssrutan om du vill tillåta åtkomst till den enhetsklassen eller specifika enheten.

   Om en kryssruta är nedtonad, har värden som påverkar åtkomstscenariot ändrats inifrån vyn Device Class Configuration (Enhetsklasskonfiguration). Du återställer värdena tillbaka till enkla inställningar genom att klicka i kryssrutan så att den avmarkeras eller markeras och sedan bekräfta med **Yes** (Ja).
3. Klicka på ikonen **Save** (Spara).

   OBS! Om ingen bakgrundstjänst är igång, öppnas en dialogruta som frågar om du vill starta den. Klicka på **Yes** (Ja).
4. Klicka på **OK**.

Starta bakgrundstjänst

Innan du kan tillämpa enhetsprofiler, öppnar HP ProtectTools Security Manager en dialogruta som frågar om du vill starta bakgrundstjänsten HP ProtectTools Device Locking/Auditing (HP ProtectTools enhetslåsning/granskning). Klicka på **Yes** (Ja). Bakgrundstjänsten startar och startas därefter alltid automatiskt när systemet startar.

OBS! En enhetsprofil måste vara definierad för att bakgrundstjänsten ska visas.

Administratörer kan också starta eller stoppa den här tjänsten:

1. Klicka på **Start** och sedan på **Kontrollpanelen**.
2. Klicka **Administrativa verktyg** och sedan på **Tjänster**.
3. Sök efter tjänsten **HP ProtectTools Device Locking/Auditing** (HP ProtectTools enhetslåsning/granskning).

Att stoppa tjänsten för enhetslåsning/granskning stoppar inte låsningen av en enhet. Två komponenter tvingar fram låsning av en enhet:

- Tjänsten för enhetslåsning/granskning
- Drivrutinen DAMDrv.sys

När du startar tjänsten startar också enhetsdrivrutinen, men att stoppa tjänsten stoppar inte drivrutinen.

Om du vill ta reda på om bakgrundstjänsten körs eller inte, öppnar du ett kommandotolksfönster och skriver sedan sc query flcdlock.

Om du vill ta reda på om enhetsdrivrutinen körs eller inte, öppnar du ett kommandotolksfönster och skriver sedan sc query damdrv.

Enhetsklasskonfiguration

Administratörer och auktoriserade användare kan visa och modifiera listor med användare och grupper som har tillåtits eller nekats åtkomst till klasser med enheter eller specifika enheter.

OBS! För att användaren eller gruppen ska kunna använda den här vyn för att läsa information om enhetsåtkomst, måste användaren eller gruppen ges "läsåtkomst" i vyn **User Access Settings** (Inställningar för användaråtkomst). För att användaren eller gruppen ska kunna visa eller modifiera information om enhetsåtkomst, måste användaren eller gruppen ges "ändringsåtkomst" i vyn **User Access Settings** (Inställningar för användaråtkomst).

Vyn Device Class Configuration (Enhetsklasskonfiguration) innehåller följande sektioner:

- **Device List** (Enhetslista) – Visar alla enhetsklasser och enheter som är installerade i systemet eller som kan ha varit installerade.
  - Skydd gäller vanligtvis för en enhetsklass. En användare eller grupp som markerats kommer att få åtkomst till alla enheter i enhetsklassen.
  - Skydd kan också tillämpas på specifika enheter.
- **User List** (Användarlista) – Visar alla användare och grupper som har tillåtits eller nekats åtkomst till den markerade enhetsklassen eller specifika enheten.
  - Posten User List (Användarlista) kan göras för en specifik användare eller för en grupp där användaren är medlem.
  - Om en användar- eller gruppost i User List (Användarlista) inte är tillgänglig har inställningen följt med enhetsklassen i Device List (Enhetslista) eller från mappen Class (Klass).
  - Vissa enhetsklasser, t.ex. DVD och CD-ROM, kan kontrolleras ytterligare genom att man tillåter eller nekar åtkomst separat för läs- och skrivoperationer.

Liksom för andra enheter och klasser kan läs- och skrivåtkomst vara inbyggd. Läsåtkomst kan t.ex. följa med från en högre klass, medan skrivåtkomst kan vara specifikt nekad för en användare eller grupp.

OBS! Om kryssrutan Read (Läs) är tom, har åtkomstkontrollposten ingen effekt på läsåtkomsten till enheten. Den varken tillåter eller nekar läsåtkomst till enheten.

Exempel 1 – Om en användare eller grupp nekas skrivåtkomst till en enhet eller klass med enheter:

Samma användare, samma grupp eller en medlem i samma grupp kan ges skrivåtkomst eller läs- och skrivåtkomst enbart för en enhet under denna enhet i enhetshierarkin.

Exempel 2 – Om en användare eller grupp ges skrivåtkomst till en enhet eller klass med enheter:

Samma användare, samma grupp eller en medlem i samma grupp kan nekas skrivåtkomst eller läs- och skrivåtkomst enbart för samma enhet eller enhet under denna enhet i enhetshierarkin.

Exempel 3 – Om en användare eller grupp ges läsåtkomst till en enhet eller klass med enheter:

Samma användare, samma grupp eller en medlem i samma grupp kan nekas läsåtkomst eller läs- och skrivåtkomst enbart för samma enhet eller enhet under denna enhet i enhetshierarkin.

Exempel 4 – Om en användare eller grupp nekas läsåtkomst till en enhet eller klass med enheter:

Samma användare, samma grupp eller en medlem i samma grupp kan ges läsåtkomst eller läs- och skrivåtkomst enbart för en enhet nedanför denna enhet i enhetshierarkin.

Exempel 5 – Om en användare eller grupp ges läs- och skrivåtkomst till en enhet eller klass med enheter:

Samma användare, samma grupp eller en medlem i samma grupp kan nekas skrivåtkomst eller läs- och skrivåtkomst enbart för samma enhet eller enhet under denna enhet i enhetshierarkin.

Exempel 6 – Om en användare eller grupp nekas läs- och skrivåtkomst till en enhet eller klass med enheter:

Samma användare, samma grupp eller en medlem i samma grupp kan ges läsåtkomst eller läs- och skrivåtkomst enbart för en enhet under denna enhet i enhetshierarkin.

Neka åtkomst för en användare eller grupp

Så här förhindrar du att en användare eller grupp kommer åt en enhet eller klass med enheter:

1. Klicka på **Device Access Manager** i den vänstra rutan i **HP ProtectTools Administrative Console** och klicka sedan på **Device Class Configuration** (Enhetsklasskonfiguration).
2. Klicka i enhetslistan på enhetsklassen du vill konfigurera.
   - Enhetsklass
   - Alla enheter
   - Enskild enhet

3. Klicka på användaren eller gruppen som ska nekas åtkomst under **User/Groups** (Användare/grupper).
4. Klicka på **Deny** (Neka) vid en användare eller grupp.
5. Klicka på ikonen **Save** (Spara).

OBS! När inställningarna för neka och tillåt är inställda på samma enhetsnivå för en användare, gäller nekad åtkomst före tillåten åtkomst.

Tillåta åtkomst för en användare eller grupp

Så här ger du en användare eller grupp åtkomst till en enhet eller klass med enheter:

1. Klicka på **Device Access Manager** i den vänstra rutan i **HP ProtectTools Administrative Console** och klicka sedan på **Device Class Configuration** (Enhetsklasskonfiguration).
2. Klicka på något av följande i enhetslistan:
   - Enhetsklass
   - Alla enheter
   - Enskild enhet
3. Klicka på **Add** (Lägg till).

   Diaglogrutan **Select Users or Groups** (Välj användare eller grupper) öppnas.
4. Klicka på **Advanced** (Avancerat) och sedan på **Find Now** (Sök nu) och leta efter användare eller grupper att lägga till.
5. Klicka på en användare eller grupp som ska läggas till i listan med tillgängliga användare och grupper och klicka sedan på **OK**.
6. Klicka på **OK** igen.
7. Klicka på **Allow** (Tillåt) om du vill ge denna användare eller grupp åtkomst.
8. Klicka på ikonen **Save** (Spara).

Ta bort åtkomst för en användare eller grupp

Så här tar du bort en användares eller grupps åtkomst till en enhet eller klass med enheter:

1. Klicka på **Device Access Manager** i den vänstra rutan i **HP ProtectTools Administrative Console** och klicka sedan på **Device Class Configuration** (Enhetsklasskonfiguration).
2. Klicka i enhetslistan på enhetsklassen du vill konfigurera.
   - Enhetsklass
   - Alla enheter
   - Enskild enhet
3. Klicka på den användare eller grupp du vill ta bort under **User/Groups** (Användare/grupper) och klicka sedan på **Remove** (Ta bort).
4. Klicka på ikonen **Save** (Spara).

Tillåta åtkomst till en klass med enheter för en användare i en grupp

Så här tillåter du åtkomst för en användare till en klass med enheter, samtidigt som du nekar åtkomst för alla andra medlemmar i den användargruppen:

1. Klicka på **Device Access Manager** i den vänstra rutan i **HP ProtectTools Administrative Console** och klicka sedan på **Device Class Configuration** (Enhetsklasskonfiguration).
2. Klicka i enhetslistan på enhetsklassen du vill konfigurera.
   - Enhetsklass
   - Alla enheter
   - Enskild enhet
3. Lägg till gruppen som ska nekas åtkomst under **User/Groups** (Användare/grupper) och klicka sedan på **Deny** (Neka).
4. Navigera till mappen under klassen som krävs och lägg sedan till den specifika användaren.
5. Klicka på **Allow** (Tillåt) för att bevilja denna användare åtkomst.
6. Klicka på ikonen **Save** (Spara).

Tillåta åtkomst till en specifik enhet för en användare i en grupp

Administratörer kan tillåta att en användare får åtkomst till en specifik enhet medan alla övriga medlemmar i den användarens grupp nekas åtkomst.

1. Klicka på **Device Access Manager** i den vänstra rutan i **HP ProtectTools Administrative Console** och klicka sedan på **Device Class Configuration** (Enhetsklasskonfiguration).
2. Klicka i enhetslistan på den enhetsklass du vill konfigurera och navigera sedan till mappen under den.
3. Klicka på **Add** (Lägg till). Diaglogrutan **Select Users or Groups** (Välj användare eller grupper) öppnas.
4. Klicka på **Advanced** (Avancerat) och klicka sedan på **Find Now** (Sök nu) så att du kan söka efter den användargrupp som ska nekas åtkomst till alla enheter i klassen.
5. Klicka på gruppen och sedan på **OK**.
6. Navigera till den specifika enhet under enhetsklassen som användaren ska få åtkomst till.
7. Klicka på **Add** (Lägg till). Diaglogrutan **Select Users or Groups** (Välj användare eller grupper) öppnas.
8. Klicka på **Advanced** (Avancerat) och sedan på **Find Now** (Sök nu) och leta efter användare eller grupper att lägga till.
9. Klicka på användaren som ska tillåtas åtkomst och klicka sedan på **OK**.
10. Klicka på **Allow** (Tillåt) för att bevilja denna användare åtkomst.
11. Klicka på ikonen **Save** (Spara).

Återställa konfigurationen

△ **VIKTIGT:** Om du återställer konfigurationen ignoreras alla ändringar i enhetskonfigurationer som har gjorts och alla inställningar återställs till fabriksinställningen.

Så här återställer du konfigurationsinställningarna till fabriksinställningen:

1. Klicka på **Device Access Manager** i den vänstra rutan i **HP ProtectTools Administrative Console** och klicka sedan på **Device Class Configuration** (Enhetsklasskonfiguration).
2. Klicka på knappen **Reset** (Återställ).
3. Bekräfta med **Yes** (Ja).
4. Klicka på ikonen **Save** (Spara).

Avancerade uppgifter

Kontrollera åtkomst till konfigurationsinställningar

I vyn **User Access Settings** (Inställningar för användaråtkomst) specificerar administratörer de grupper eller användare som tillåts använda sidorna Simple Configuration (Enkel konfiguration) och Device Class Configuration (Enhetsklasskonfiguration).

OBS! En användare eller grupp måste ha "full administratörsbehörighet för användare" för att kunna modifiera inställningarna i vyn User Access Settings (Inställningar för användaråtkomst).

- En användare eller grupp måste ges åtkomst av typen "visa (endast läsning) konfigurationsinställningar" i vyn User Access Settings (Inställningar för användaråtkomst) för att kunna visa information från Simple Configuration (Enkel konfiguration) och Device Class Configuration (Enhetsklasskonfiguration).
- En användare eller grupp måste ges åtkomst av typen "ändra konfigurationsinställningar" i vyn User Access Settings (Inställningar för användaråtkomst) för att kunna ändra information från Simple Configuration (Enkel konfiguration) och Device Class Configuration (Enhetsklasskonfiguration).

OBS! Även medlemmar i gruppen Administratörer måste ha "läsåtkomst" för att kunna visa vyerna Simple Configuration (Enkel konfiguration) och Device Class Configuration (Enhetsklasskonfiguration) och ha "ändringsåtkomst" för att kunna ändra data med vyerna Simple Configuration och Device Class Configuration.

OBS! Om en användare efter en utvärdering av åtkomstnivåerna för alla användare och grupper inte har "tillåt" eller "neka" för en viss åtkomstnivå, nekas användaren åtkomst på den nivån.

Tillåta åtkomst för en befintlig grupp eller användare

Så här tillåter du att en befintlig grupp eller användare visar eller ändrar konfigurationsinställningarna:

1. Klicka på **Device Access Manager** i den vänstra rutan i **HP ProtectTools Administrative Console** och klicka sedan på **User Access Settings** (Inställningar för användaråtkomst).
2. Klicka på en grupp eller användare som ska ges åtkomst.
3. Under **Permissions** (Behörigheter), klicka på **Allow** (Tillåt) för varje typ av behörighet som ska tillåtas för den valda gruppen eller användaren:

   OBS! Behörigheterna ges kumulativt. En användare som exempelvis har behörighet att ändra konfigurationsinställningar får automatiskt behörighet att visa (endast läsning) konfigurationsinställningar. En användare som har full behörighet som användaradministratör ges också behörighet att ändra konfigurationsinställningar och visa (endast läsning) konfigurationsinställningar.

   - Full behörighet för användaradministratör
   - Ändra konfigurationsinställningar
   - Visa (endast läsning) konfigurationsinställningar
4. Klicka på ikonen **Save** (Spara).

Neka åtkomst för en befintlig grupp eller användare

Så här nekar du att en befintlig grupp eller användare visar eller ändrar konfigurationsinställningarna:

1. Klicka på **Device Access Manager** i den vänstra rutan i **HP ProtectTools Administrative Console** och klicka sedan på **User Access Settings** (Inställningar för användaråtkomst).
2. Klicka på en grupp eller användare som ska nekas åtkomst.
3. Under **Permissions** (Behörigheter), klicka på **Deny** (Neka) för varje typ av behörighet som ska nekas för den valda gruppen eller användaren:
   - Full behörighet för användaradministratör
   - Ändra konfigurationsinställningar
   - Visa (endast läsning) konfigurationsinställningar
4. Klicka på ikonen **Save** (Spara).

Lägga till en ny grupp eller användare

Så här tillåter du att en ny grupp eller användare visar eller ändrar konfigurationsinställningarna:

1. Klicka på **Device Access Manager** i den vänstra rutan i **HP ProtectTools Administrative Console** och klicka sedan på **User Access Settings** (Inställningar för användaråtkomst).
2. Klicka på **Add** (Lägg till). Diaglogrutan **Select Users or Groups** (Välj användare eller grupper) öppnas.
3. Klicka på **Advanced** (Avancerat) och sedan på **Find Now** (Sök nu) och leta efter användare eller grupper att lägga till.
4. Klicka på en grupp eller användare, klicka på **OK** och klicka sedan på **OK** igen.
5. Klicka på **Allow** (Tillåt) för att bevilja denna användare åtkomst.
6. Klicka på ikonen **Save** (Spara).

Ta bort åtkomst för grupp eller användare

Så här tar du bort behörigheten för en grupp eller användare att visa eller ändra konfigurationsinställningarna:

1. Klicka på **Device Access Manager** i den vänstra rutan i **HP ProtectTools Administrative Console** och klicka sedan på **User Access Settings** (Inställningar för användaråtkomst).
2. Klicka på en grupp eller användare och klicka sedan på **Remove** (Ta bort).
3. Klicka på ikonen **Save** (Spara).

Relaterad dokumentation

Device Access Manager för HP ProtectTools är kompatibelt med företagsprodukten HP ProtectTools Enterprise Device Access Manager. Tillsammans med företagsprodukten ger Device Access Manager för HP ProtectTools endast läsåtkomst till sina egna funktioner.

Mer information om Device Access Manager för HP ProtectTools finns på webben på http://www.hp.com/hps/security/products.

12 LoJack Pro för HP ProtectTools

Med Absolute Softwares Computrace-produkter kan användarna spåra sina HP-datorer och förbättra dataskyddet. Computrace LoJack-produkterna minskar även datorförlusterna och hjälper till att återfinna stulna datorer.

Gör så här om du vill aktivera Computrace-produkten:

1. Klicka på **Start**, **Alla program** och **HP ProtectTools Security Manager**.
2. Klicka på **Theft Recovery** (Återfinn vid stöld) och klicka på **Activate Now** (Aktivera nu).

   Din standardwebbläsare öppnar en abonnemangssida där du kan välja en av de tre Computrace-produkter som är tillgängliga med HP ProtectTools:

   - **Computrace Data Delete** – Omfattar fjärradering av data, frysning av enheter och grundläggande inventariespårning och -rapportering.
   - **Computrace LoJack Pro** – Omfattar fjärradering av data, frysning av enheter, grundläggande inventariespårning och -rapportering samt administrerad eftersökning vid stöld.
   - **Computrace LoJack Pro Premium** – Omfattar fjärradering av data, frysning av enheter, grundläggande inventariespårning och -rapportering, geolocation och geofencing samt administrerad eftersökning vid stöld.

Computrace Agent är inbyggd i BIOS på HP Business Notebook-datorer, men denna Agent är avstängd vid leveransen av datorn. När du har köpt ditt abonnemang kan Agent aktiveras. Denna inbyggda Agent kan installera om operativsystemet och formatera om hårddiskarna.

OBS! Abonnemangsperioder från 1 till 5 år är tillgängliga. I avtalet för programvaruabonnemang från Absolute finns mer information. Eftersökningsfunktionen är beroende av den geografiska platsen. GPS-spårning stöds på vissa modeller med WWAN-tillvalet.

13 Felsökning

HP ProtectTools Security Manager

Kort beskrivning	Detaljer	Lösning
Smart card-kort och USB-säkerhetskort är inte tillgängliga i Security Manager om de installerades senare än Security Manager.	För att du ska kunna använda smartcard-kort eller USB-säkerhetskort i Security Manager måste stödprogramvaran (drivrutiner, PKCS#11-gränssnitt osv.) installeras före Security Manager. Om du redan har installerat Security Manager kan du göra så här när du har installerat stödprogramvaran för smart card-kort eller säkerhetskort:	Logga in i Password Manager. I HP ProtectTools Security Manager klickar du på **Password Manager** (Lösenordshanteraren), klickar på **Credentials** (Autentiseringsuppgifter) och klickar sedan på **Smart Card**. Starta om datorn om du uppmanas till det.
Vissa programwebbplatser skapar fel som hindrar användaren att utföra eller slutföra uppgifter.	Vissa webbaserade program slutar att fungera och rapporterar fel pga det inaktiverade funktionsmönstret i enkel inloggning. Ett **!** i en gul triangel kan t ex visas i Internet Explorer för att indikera att ett fel har inträffat.	Security Manager Single Sign On stöder inte alla programvarugränssnitt för webben. Inaktivera stödet för Single Sign On för den specifika webbsidan genom att stänga av det. Se vidare den kompletta dokumentationen om Single Sign On, som finns i Security Managers programvaruhjälp. Om en särskild enkel inloggning inte kan inaktiveras för ett givet program, kan du ringa HP:s tekniska support och begära tredjenivåsupport via din HP Service-kontakt.
Alternativet **Browse for Virtual Token** (Bläddra efter virtuellt kort) visas inte under inloggningsprocessen.	Användaren kan inte flytta ett registrerat virtuellt kort i Password Manager, eftersom alternativet för bläddring har tagits bort för att ge högre säkerhet.	Bläddringsalternativet togs bort eftersom det tillät icke-användare att ta bort och byta namn på filer och ta kontroll över Windows.
Domänadministratörer kan inte ändra Windows-lösenord ens om de har behörighet till det.	Detta inträffar när en domänadministratör loggar in på en domän och registrerar domänidentiteten med hjälp av Password Manager och ett konto med administratörsrättigheter i domänen och på den lokala PC:n. När domänadministratören försöker ändra Windows-lösenordet från Password Manager, får han eller hon ett felmeddelande: **User account restriction** (Begränsningar för användarkonto).	Password Manager kan inte ändra ett användarlösenord till en domän med **Change Windows password** (Ändra Windows-lösenord). Security Manager kan bara ändra den lokala PC:ns kontolösenord. Domänanvändaren kan ändra sitt lösenord via alternativet **Ändra lösenord** i **Säkerhet för Windows**, men eftersom domänanvändaren inte har något fysiskt konto på den lokala PC:n kan Password Manager bara ändra det lösenord som används för inloggning.
Password Manager har inkompatibilitetsproblem med lösenordets GINA i Corel WordPerfect 12.	Om användaren loggar in i Password Manager, skapar ett dokument i WordPerfect och sparar detta med lösenordsskydd, kan Password Manager inte detektera eller känna igen	HP undersöker om det finns en workaround för framtida produktförbättringar.

Kort beskrivning	Detaljer	Lösning
	lösenordets GINA, varken manuellt eller automatiskt.	
Password Manager känner inte igen knappen **Connect** (Anslut) på skärmen.	Om behörighetskontrollerna för enkel inloggning för Remote Desktop Connection (RDP, datorfjärranslutning) ställs in till **Connect** när enkel inloggning startas om, anger den alltid **Save As** (Spara som) istället för **Connect**.	HP undersöker om det finns en workaround för framtida produktförbättringar.
Användaren kan inte logga in i Password Manager efter en övergång från vänteläge till viloläge (gäller enbart Windows XP Service Pack 1).	När systemet har tillåtits övergå till viloläge och sömnläge, kan administratören eller användaren inte logga in i Password Manager och Windows inloggningsskärm fortsätter att visas oavsett vilka autentiseringsuppgifter som väljs för inloggning (lösenord, fingeravtryck eller Java Card-kort).	Uppdatera Windows till Service Pack 2 via Windows Update. I artikel 813301 i Microsofts kunskapsdatabas på http://www.microsoft.com finns mer information om orsaken till detta. Frö att kunna logga in måste användaren välja Password Manager och logga in. Efter inloggning i Password Manager uppmanas användaren att logga in i Windows (användaren måste eventuellt välja Windows inloggningsalternativ) för att slutföra inloggningsprocessen. Om användaren loggar in i Windows först, måste användaren logga in i Password Manager manuellt.
Säkerhetsprocessen **Restore Identity** (Återställ identitet) förlorar sin association med det virtuella kortet.	När användaren återställer identiteten, kan Password Manager förlora associationen till platsen där det virtuella kortet finns på inloggningsskärmen. Även om Password Manager har det virtuella kortet registrerat, måste användaren registrera om kortet för att återställa associationen.	Så fungerar systemet för närvarande. Om man avinstallerar Security Manager utan att behålla identiteterna förstörs kortets systemdel (serverdel) så att kortet inte längre kan användas för inloggning, även om kortets klientdel återställs genom identitetsåterställning. HP undersöker lösningsalternativ som kan fungera även på sikt.

Device Access Manager for HP ProtectTools

Användare har nekats åtkomst till enheter inom Device Access Manager, men enheterna kan fortfarande nås.

- **Förklaring** – Simple Configuration (Enkel konfiguration) och/eller Device Class Configuration (Enhetsklasskonfiguration) har använts inom Device Access Manager för att neka användare åtkomst till enheter. Trots att användarna nekats åtkomst, kan de fortfarande komma åt enheterna.
- **Lösning:**
  - Verifiera att tjänsten HP ProtectTools Device Locking (HP ProtectTools enhetslåsning) har startats.
  - Som administrativ användare klickar du på **Kontrollpanelen** och sedan på **System och underhåll**. I fönstret Administrativa verktyg klickar du på **Tjänster** söker du efter tjänsten **HP ProtectTools Device Locking/Auditing** (Låsning/granskning av HP ProtectTools-enhet). Kontrollera att tjänsten startas och att starttypen är **Automatisk**.

En användare har oväntat fått åtkomst till en enhet, eller en användare har oväntat nekats åtkomst till en enhet.

- **Förklaring** – Man har använt Device Access Manager för att neka användare åtkomst till vissa enheter och tillåta åtkomst till andra enheter. När användarna använder systemet, kan de komma åt enheter som de tror att Device Access Manager har nekat dem åtkomst till. De kan också nekas åtkomst till enheter som de tror att Device Access Manager borde tillåta åtkomst till.
- **Lösning:**
  - Kontrollera användarens enhetsinställningar med Device Class Configuration (Enhetsklasskonfiguration) i Device Access Manager.
  - Klicka på **Security Manager**, klicka på **Device Access Manager** och klicka sedan på **Device Class Configuration**. Visa nivåerna i Device Class-trädet och granska de inställningar som gäller den här användaren. Leta efter eventuella markeringar med "Deny" (Neka) som kan vara inställda för användaren eller någon Windows-grupp där han eller hon kan vara medlem, t.ex. Användare eller Administratörer.

Tillåta eller neka – vilket går före?

- **Explanation** (Förklaring) – Inom Device Class-konfigurationen har följande konfiguration ställts in:
  - En Windows-grupp (t.ex. BUILTIN\Administrators) har fått behörigheten Tillåt och en annan Windows-grupp (t.ex. BUILTIN\Users) har fått behörigheten Neka på samma nivå i enhetsklasshierarkin (t.ex. DVD/CD-ROM-enheter).
  - Om en användare är medlem i båda dessa grupper (t.ex. Administratör), vilken gäller först?
- **Lösning:**
  - Användaren nekas åtkomst till enheten. Nekad åtkomst går före tillåten.
  - Åtkomst nekas på grund av hur Windows räknar ut den faktiska behörigheten för enheten. En grupp nekas och en grupp tillåts, men användaren är medlem i båda grupperna. Användaren nekas eftersom nekad åtkomst går före tillåten.

- Ett sätt att undvika detta är att neka gruppen Användare på DVD/CD-ROM-enhetsnivå och tillåta gruppen Administratörer på nivån under DVD/CD-ROM-enheter.
- En alternativ lösning är att skapa specifika Windows-grupper, en för att tillåta åtkomst till DVD/CD och en för att neka åtkomst till DVD/CD. Specifika användare skulle då läggas till i rätt grupp.

Man har använt vyn Simple Configuration (Enkel konfiguration) för att definiera en princip för kontroll av enhetsåtkomst, men administrativa användare kan inte nå enheterna.

- **Förklaring** – Simple Configuration (Enkel konfiguration) nekar åtkomst för användare och gäster, och tillåter enhetsadministratörer.
- **Lösning:** Lägg till den administrativa användaren i gruppen Enhetsadministratörer.

Diverse

Programvarupåverkan —Kort beskrivning	Detaljer	Lösning
Security Manager—varning mottagen: **The security application can not be installed until the HP Protect Tools Security Manager is installed** (Säkerhetsprogrammet kan inte installeras förrän HP ProtectTools Security Manager har installerats.)	Alla säkerhetsprogram som Java Card Security och biometrisk teknik är utökningsbara plugin-program för Security Managers gränssnitt. Security Manager måste vara installerat innan ett HP-godkänt plugin-säkerhetsprogram kan laddas.	Programvaran Security Manager måste installeras innan något säkerhetsplugin-program kan installeras.
HP ProtectTools Security Manager—Ett fel returneras periodiskt när gränssnittet Security Manager stängs.	Periodvis (1 av 12 gånger) skapas ett fel när stängningsknappen i det övre högra hörnet av skärmen används för att stänga Security Manager innan alla plugin-program har slutfört sina inläsningar.	Detta är relaterat till ett tidsberoende för plugin-tjänsters inläsningstid när Security Manager stängs och startas om. Eftersom PTHOST.exe är det shell-program som håller i de andra programmen (plugin-program), beror det på plugin-programmets möjlighet att slutföra sin inläsningstid (tjänster). Stängs shell-programmet innan plugin-programmet fått tid att slutföra inläsningen är detta kärnan till problemet. Tillåt Security Manager att slutföra inläsningen av tjänsten (syns överst i Security Managerfönstret) och alla plugin-program som listas i den vänstra kolumnen.
HP ProtectTools—Obegränsad åtkomst eller okontrollerade administratörsrättigheter utgör en säkerhetsrisk.	Det finns ett antal möjliga risker med obegränsad åtkomst till klientdatorn, inklusive följande: • Borttagning av PSD • Skadliga ändringar av användarinställningar • Inaktivering av säkerhetspolicies och funktioner	Administratörer uppmuntras att tillämpa "bästa praxis" när det gäller att begränsa slutanvändarnas privilegier och användarnas åtkomst. Obehöriga användare bör inte ges administratörsprivilegier.

Ordlista

administratör *Se* Windows-administratör.

aktivering Den aktivitet som måste utföras innan en funktion i Drive Encryption blir tillgänglig. Drive Encryption aktiveras med HP ProtectTools Setup Wizard. Det är bara en administratör som kan aktivera Drive Encryption. Aktiveringen består av att aktivera programvaran, kryptera enheten, skapa ett användarkonto och skapa den inledande krypteringsnyckeln i en flyttbar lagringsenhet.

användare Person som är registrerad i Drive Encryption. Användare som inte är administratörer har begränsade rättigheter i Drive Encryption. De kan bara registrera sig (efter administratörens godkännande) och logga in.

arkiv för akut återställning Skyddat lagringsområde som tillåter omkryptering av grundläggande användarnycklar från en plattformsägarnyckel till en annan.

ATM Automatic Technology Manager, som gör att nätverksadministratörer kan administrera system på distans på BIOS-nivå.

auktoriserad användare En användare som har fått behörighet i vyn User Access Settings (Inställningar för användaråtkomst) att visa eller modifiera konfigurationsinställningar i vyn Simple Configuration (Enkel konfiguration) eller Device Class Configuration (Enhetsklasskonfiguration).

autentisering Process då man verifierar att en användare är behörig att utföra en uppgift som t.ex. att använda en dator, ändra inställningar för ett visst program eller visa skyddade data.

autentisering vid start Säkerhetsfunktion som kräver någon form av autentisering, t ex ett Java Card-kort, säkerhetschip eller lösenord när datorn sätts på.

automatisk shredding Schemalagd shredding-procedur som användaren ställer in i File Sanitizer.

bakgrundstjänst Bakgrundstjänsten HP ProtectTools Device Locking/Auditing (HP ProtectTools enhetslåsning/granskning), som måste köras för att principerna för kontroll av enhetsåtkomst ska kunna tillämpas. Den kan ses inifrån programmet Tjänster under alternativet Administrativa verktyg på Kontrollpanelen. Om den inte körs, försöker HP ProtectTools Security Manager att starta den när principerna för kontroll av enhetsåtkomst tillämpas.

behörighetskontroller Metod genom vilken en användare bevisar sin lämplighet för en särskild uppgift i autentiseringsprocessen.

betrodd avsändare En betrodd kontakt som skickar signerad och/eller krypterad e-post och Microsoft Office-dokument.

betrodd kontakt En person som har tackat ja till att vara betrodd kontakt.

biometrisk Kategori av behörighetskontroll som använder en fysisk funktion, t ex ett fingeravtryck, för att identifiera en användare.

certifierande myndighet Tjänst som utfärdar de certifikat som behövs för att köra en allmän nyckelinfrastruktur.

chatthistoriksession Krypterad fil som innehåller en post med båda sidorna av en konversation i en chattsession.

cryptographic service provider (CSP) Leverantör eller bibliotek för kryptografiska algoritmer som kan användes i ett väldefinierat gränssnitt för att utföra särskilda kryptografiska funktioner.

dekryptering Procedur som används i kryptografi för att konvertera krypterad data till vanlig text.

digital signatur Data som skickats med en fil som verifierar avsändaren av materialet och intygar att filen inte har ändrats efter signeringen.

digitalt certifikat Elektroniska behörighetskontroller som bekräftar en individs eller ett företags identitet genom att binda det digitala certifikatets ägares identitet till ett par elektroniska nycklar som används för signering av digital information.

domän Grupp med datorer som utgör en del av ett nätverk med en gemensam katalogdatabas. Domäner har unika namn och varje domän har en uppsättning gemensamma regler och procedurer.

Drive Encryption Skyddar data genom att kryptera en eller flera hårddiskar, och göra informationen oläslig för personer som saknar rätt behörighet.

DriveLock Säkerhetsfunktion som länkar hårddisken till en användare och kräver att användaren skriver rätt DriveLock-lösenord när datorn startar.

Encryption File System (EFS), krypteringsfilsystem System som krypterar alla filar och undermappar i den valda mappen.

enhetsklass Alla enheter av en viss typ, t.ex. diskar.

enkel inloggning Funktion som sparar autentiseringsinformation och låter dig använda Security Manager för att komma åt Internet- och Windows-program som kräver lösenordsidentifiering.

fingeravtryck En digital extrahering av din fingeravtrycksbild. Din faktiska fingeravtrycksbild lagras aldrig av Security Manager.

free space bleaching Säker metod som skriver över raderade objekt med slumpmässigt utvalda data, som förvränger innehållet i det raderade objektet.

försegla åt betrodda kontakter En aktivitet som lägger till en digital signatur i ett e-postmeddelande, krypterar det och skickar det så snart du autentiserat dig med önskad metod för säker inloggning.

grupp En grupp användare som har samma nivå av åtkomst eller nekad åtkomst till en enhetsklass eller en specifik enhet.

HP SpareKey Säkerhetskopia av Drive Encryption-nyckel.

identitet En grupp av behörighetskontroller och inställningar i HP ProtectTools Security Manager som hanteras som ett konto eller en profil för en särskild användare.

ID-kort En gadget på Sidpanelen i Windows som är avsedd att visuellt identifiera ditt skrivbord med ditt användarnamn och den bild du valt. Klicka på ID-kortet, så öppnas HP ProtectTools Administrative Console.

inbjudan till betrodd kontakt Ett e-postmeddelande som skickas till en person som ombeds att bli betrodd kontakt.

inloggning Ett objekt i Security Manager som består av ett användarnamn och lösenord (och eventuellt annan vald information) som man kan använda för att logga in på webbplatser eller i andra program.

inloggningsbild för Drive Encryption En inloggningsbild som visas innan Windows startar. Användaren måste ange sitt användarnamn, sitt lösenord eller sin Java Card-PIN-kod i Windows. I de flesta fall kommer man in direkt

i Windows utan att logga in igen i Windows inloggningsbild, om man anger rätt information i Drive Encryptions inloggningsbild.

instrumentpanel En central punkt varifrån du kan nå och administrera funktionerna och inställningarna i Security Manager for HP ProtectTools.

Java Card Ett uttagbart kort som sitter i datorn och innehåller identifierande information för inloggning. För att du ska kunna logga in med ett Java Card-kort på inloggningsbilden i Drive Encryption måste du sätta i Java Card-kortet och skriva ditt användarnamn och din Java Card-PIN-kod.

knappen Send Security (Skicka säkert) En knapp i programvaran som visas i verktygsfältet i e-postmeddelanden i Microsoft Outlook. Genom att klicka på knappen kan du signera och/eller kryptera ett e-postmeddelande i Microsoft Outlook.

knappen Sign and Encrypt (Signera och kryptera) En knapp i programvaran som visas i verktygsfältet i Microsoft Office-program. Genom att klicka på knappen kan du signera, kryptera eller ta bort kryptering i ett Microsoft Office-dokument.

konsol En central punkt varifrån du kan nå och administrera funktionerna och inställningarna i HP ProtectTools Administrative Console.

kryptering Procedur, t ex användningen av en algoritm, som nyttjas i kryptografi för att konvertera vanlig text till chiffrerad text i avsikt att hindra obehöriga mottagare från att läsa dessa data. Det finns många typer av datakryptering, och de utgör grunden för nätverkssäkerhet. Vanliga typer inkluderar Data Encryption Standard och allmännyckelkryptering.

kryptografi Ett sätt att kryptera och dekryptera data så att de bara kan avkodas av särskilda personer.

lista med betrodda kontakter En lista över betrodda kontakter.

Live Messenger History Viewer En komponent i Privacy Manager Chat som gör att du kan söka efter och visa krypterade sessioner med chatthistorik.

lösenord för återkallelse Ett lösenord som skapas när en användare begär ett digitalt certifikat. Användaren måste ange lösenordet när han eller hon vill återkalla sitt digitala certifikat. Detta säkerställer att det bara är användaren som kan återkalla certifikatet.

manuell shredding Omedelbar exekvering av shredding på ett eller flera valda objekt, inte enligt det automatiska shredding-schemat.

migrering En aktivitet som gör att du kan hantera, återställa och överföra Privacy Manager-certifikat och betrodda kontakter.

mottagare av inbjudan som betrodd kontakt En person som erbjuds att bli betrodd kontakt.

nätverkskonto Windowsanvändare eller -konto, antingen på en lokal dator, i en arbetsgrupp eller på en domän.

objekt En datakomponent som består av personlig information eller personliga filer, historikdata, webbrelaterade data osv. som finns på hårddisken.

PIN-kod Personal identification number (personligt identifikationsnummer).

PKI Public Key Infrastructure, en standard som definierar gränssnitten för att skapa, använda och administrera certifikat och kryptografiska nycklar.

princip för kontroll av enhetsåtkomst Listan med enheter till vilka en användare tillåts eller nekas åtkomst.

Privacy Manager-certifikat Ett digitalt certifikat som kräver autentisering varje gång du använder det för kryptografi, t.ex. signering och kryptering av e-postmeddelanden och Microsoft Office-dokument.

PSD Personal Secure Drive, som ger ett skyddat lagringsutrymme för känslig information.

SATA device mode (SATA-enhetsläge) Dataöverföringsläge mellan en dator och datalagringsenheter, t.ex. hårddiskar och optiska enheter.

scen Ett fotografi av en registrerad användare att använda för autentisering.

shredding Exekvering av en algoritm som döljer informationen i ett objekt.

shredding-cykel Hur många gånger shredding-algoritmen ska exekveras på varje objekt. Ju fler shredding-cykler du väljer, desto säkrare blir datorn.

shredding-profil En specifik raderingsmetod och lista med objekt.

signaturrad En platshållare som visar var den digitala signaturen hamnar. När ett dokument signeras, visas signatursättarens namn och verifieringsmetod. Signeringsdatumet och signatursättarens titel kan också visas.

signatursättare En användare som är utsedd av ägaren av ett Microsoft Word- eller Microsoft Excel-dokument att lägga till en signaturrad i dokumentet.

simple delete Radering av Windows-referens till ett objekt. Objektet finns kvar på hårddisken tills den dolda informationen skrivs över med free space bleaching.

smart card En liten maskinvara, av ungefär samma form och storlek som ett kreditkort, som lagrar identifieringsinformation om ägaren. Används för att autentisera en dators ägare.

starta om Processen med att starta om datorn.

säkerhetskopiering Använd säkerhetskopieringsfunktionen när du vill spara en kopia av viktig programinformation på en plats utanför programmet. Den kan användas för återställning av informationen senare på samma dator eller en annan.

säkerhetskort Se metod för säker inloggning.

säker IM-kommunikation En kommunikationssession då säkra meddelanden skickas från en betrodd avsändare till en betrodd kontakt.

säker inloggningsmetod Den metod som används för inloggning på datorn.

säkert meddelande En kommunikationssession då säkra meddelanden skickas från en betrodd avsändare till en betrodd kontakt.

tangentsekvens En kombination av specifika tangenter som initierar automatisk shredding när du trycker på dem – t.ex. ctrl+alt+s.

TXT Trusted Execution Technology.

USB-kort Säkerhetsenhet som lagrar identifierande information om en användare. Liksom ett Java Card-kort eller en biometrisk läsare används det för autentisering av datorns ägare.

Windows-administratör En användare med full behörighet att ändra tillstånd och hantera andra användare.

Windows-användarkonto Profil för en person som är behörig att logga in i ett nätverk eller på en enskild dator.

Windows inloggningssäkerhet Skyddar ditt eller dina Windows-konton genom att kräva specifika autentiseringsuppgifter för åtkomst.

virtuellt kort Säkerhetsfunktion som fungerar i stort sett som ett Java Card-kort och kortläsare. Säkerhetskortet sparas antingen på datorns hårddisk eller i Windows register. När du loggar in med ett virtuellt säkerhetskort, uppmanas du att ange användar-PIN-koden så att autentiseringen kan slutföras.

visa (chatthistorik) En aktivitet som låter användaren dekryptera en eller flera chatthistoriksessioner, vilket leder till att en eller flera kontakters namn visas på skärmen med vanlig text och sessionen blir tillgänglig för visning.

återställa En process som kopierar programinformation från en tidigare sparad fil med säkerhetskopia till detta program.

Index

A

administrationsverktyg, lägga till 22
aktivera
  Drive Encryption 42
  free space bleaching 76
anpassa
  shredding-profil 71
  simple delete, profil 72
ansikte
  inställningar 17
  registrera scener 27
använda
  HP ProtectTools Administrative Console 12
användare
  neka åtkomst 81
  ta bort 82
  tillåta åtkomst 82
Applications, flikinställningar 21, 39
autentisering 14
autentiseringsuppgifter 36, 37
autentiseringsuppgifter, registrera 27
avbryta shredding eller bleaching 76

B

backup-nycklar, skapa 44
bakgrundstjänst 79
begränsa
  enhetsåtkomst 77
  åtkomst till känslig information 3
beställa ett digitalt certifikat 48
betrodda kontakter
  kontrollera återkallningsstatus 53
  lägga till 51
  radera 53
  visa detaljer 53

C

central administration 66
certifikat, förtilldelat 48
chatta i fönstret Communications (Kommunikation) 61
chatthistorik, visa 61

D

definiera
  vilka objekt som ska bekräftas före radering 72
  vilka objekt som ska bekräftas före shredding 72
dekryptera enheter 40, 44
Device Access Manager for HP ProtectTools
  felsökning 90
  öppna 78
digitalt certifikat
  beställa 48
  förnya 49
  installera 48
  radera 49
  ställa in standardvärde 49
  ta emot 48
  visa detaljer 49
  återkalla 50
  återställa 50
Discover more (Upptäck mer) 39
Drive Encryption for HP ProtectTools
  aktivera 42
  inaktivera 42
  logga in efter aktivering av Drive Encryption 42
  säkerhetskopiering och återställning 44
Drive Encryption för HP ProtectTools
  dekryptera enskilda enheter 44
  hantera Drive Encryption 44
  kryptera enskilda enheter 44
  öppna 41

E

enhet, tillåta åtkomst för användare 83
enhetsinställningar
  ansikte 17
  fingeravtryck 17
  smart card 17
  specificera 17
enhetsklass
  konfiguration 80
  tillåta åtkomst för användare 83
enkel konfiguration 78
e-posta krypterat Microsoft Office-dokument 58
e-postmeddelande
  försegla åt betrodda kontakter 55
  signera 55
  visa ett förseglat meddelande 55
Excel, lägga till signaturrad 56

F

felsökning
  Device Access Manager 90
  diverse 92
  security manager 88
File Sanitizer for HP ProtectTools
  ikon 75
  installation 70

File Sanitizer för HP ProtectTools
öppna 70
fingeravtryck
inställningar 17
registrera 27
free space bleaching 71
funktioner, HP ProtectTools 2
fördefinierad shredding-profil 71
försegla 55

G
General, flikinställningar 20
grupp
neka åtkomst 81
ta bort 82
tillåta åtkomst 82
guide
HP ProtectTools Setup 8

H
hantera
användare 16
autentiseringsuppgifter 36
lösenord 21, 31, 32
HP ProtectTools Administrative Console
använda 12
konfigurera 13
öppna 11
HP ProtectTools-funktioner 2
HP ProtectTools Security Manager
felsökning 88
installationsprocedurer 27
Lösenord till säkerhetskopiering och återställning 5
öppna 25

I
ID-kort 37
inaktivera Drive Encryption 42
information
begränsad åtkomst till 3
säkerhetskopiera 38
återställa 38
inloggning
meny 33
inloggningar
hantera 34
kategorier 34
lägga till 32
redigera 33
Installationsguide 8
instrumentpanelsinställningar 26
inställning
free space bleaching, schema 71
shredding-schema 70
inställningar
avancerade 18
avancerade användar- 29
General (Allmänt), fliken 20
ikon 35
lägga till 21
program 21
Inställningar
lägga till 26, 39
program 26, 39
inställningar, egna 37

J
Java Card Security for HP ProtectTools, PIN-kod 5

K
konfiguration
enhetsklass 80
enkel 78
inställningar 85
kontrollera åtkomst 85
återställa 84
konfigurera
enhetsåtkomst 78
HP ProtectTools Administrative Console 13
Privacy Manager för ett Microsoft Office-dokument 56
Privacy Manager för Microsoft Outlook 54
Privacy Manager för Windows Live Messenger 60
program 19
kryptera
enheter 40, 43, 44
Microsoft Office-dokument 58
krypteringsstatus, visa 43

L
logga in på datorn 42
LoJack Pro 87
lägga till
användare 86
grupp 86
signaturrad 56
signatursättare 57
signatursättares signaturrad 57
lösenord
hantera 5
HP ProtectTools 5
principer 4
riktlinjer 7
säkerhet 35
säkert 7
ändra 29

M
manuell shredding
alla markerade objekt 75
ett objekt 75
Microsoft Excel, lägga till signaturrad 56
Microsoft Office
e-posta krypterat dokument 58
kryptera ett dokument 58
signera ett dokument 56
ta bort kryptering 58
visa krypterat dokument 59
visa signerat dokument 59
Microsoft Word, lägga till signaturrad 56
mål, säkerhet 3

N
neka åtkomst 81

O
obehörig åtkomst, förhindra 3

P
Password Manager 31, 32
Privacy Manager
använda i Windows Live Messenger 59
använda med Microsoft Office 2007-dokument 55
använda med Microsoft Outlook 54
Privacy Manager-certifikat
beställa 48
förnya 49
installera 48

radera 49
ställa in standardvärde 49
ta emot 48
visa detaljer 49
återkalla 50
återställa 50
Privacy Manager for HP ProtectTools
autentiseringsmetoder 46
installation 47
migrera Privacy Manager-certifikat och betrodda kontakter till annan dator 65
säker inloggning, metoder 46
Privacy Manager för HP ProtectTools
hantera betrodda kontakter 51
hantera Privacy Manager-certifikat 47
Privacy Manager-certifikat 47
systemkrav 46
öppna 47
program, konfigurera 19

R
registrera
fingeravtryck 27
scener 27
registrera
autentiseringsuppgifter 27

S
scen
registrera 27
shredding-cykel 71
signatursättare
lägga till 57
lägga till signaturrad 57
signera
e-postmeddelande 55
Microsoft Office-dokument 56
simple delete 72
skapa
backup-nycklar 44
shredding-profil 71
skydda objekt från automatisk shredding 72
smart card
inställningar 17
specificera
säkerhetsinställningar 15
starta chattsession i Privacy Manager 60
styra enhetsåtkomst 77
stöld, skydd mot 3
systemkrav 46
säkerhet
roller 5
sammanfattning 39
viktiga mål 3
säkerhetskopiera
betrodda kontakter 65
HP ProtectTools autentiseringsuppgifter 7
information 38
Privacy Manager-certifikat 65
säkerhetsprogram, status 39
säkerhetsroller 5

T
ta bort
användaråtkomst 86
gruppåtkomst 86
kryptering från Microsoft Office-dokument 58
tangentsekvens 74
tillåta åtkomst 82

U
Uppdateringar och meddelanden 23, 39
utesluta objekt från automatisk radering 73

V
verktyg, lägga till 22
viktiga säkerhetsmål 3
visa
chatthistorik 61
förseglat e-postmeddelande 55
krypterat Microsoft Office-dokument 59
loggfiler 76
signerat Microsoft Office-dokument 59
välja
objekt för shredding 71
shredding-profil 71

W
Windows inloggningslösenord 5
Windows Live Messenger, chatta 61
Word, lägga till signaturrad 56

Å
återställa
HP ProtectTools autentiseringsuppgifter 7
information 38
Privacy Manager-certifikat och betrodda kontakter 65
återställning, utföra 45
åtkomst
förhindra obehörig 3
neka 81
neka för befintliga grupper eller användare 86
styra 77
tillåta 82
tillåta för befintliga grupper eller användare 85

Ö
öppna
Device Access Manager for HP ProtectTools 78
Drive Encryption för HP ProtectTools 41
File Sanitizer för HP ProtectTools 70
HP ProtectTools Administrative Console 11
HP ProtectTools Security Manager 25
Privacy Manager för HP ProtectTools 47