HP ProtectTools
Brugervejledning

Første udgave: November 2009

Dokumentets bestillingsnummer: 593308-081

Indholdsfortegnelse

1 Introduktion til sikkerhed

Softwaren til HP ProtectTools Security Manager indeholder sikkerhedsfunktioner, der kan bruges til at beskytte mod uautoriseret adgang til computeren, netværkene og kritiske data. Administration af HP ProtectTools Security Manager sker via funktionen Administrative Console.

Ved brug af HP ProtectTools Administrative Console kan den lokale administrator udføre følgende opgaver:

- Aktivering eller deaktivering af sikkerhedsfunktioner
- Registrering af fingeraftryk og fingeraftryk fra andre brugere af denne computer
- Registrering af et eller flere motiver til ansigtsgenkendelse
- Installation af et chipkort til godkendelse
- Angivelse af nødvendige legitimationsoplysninger til godkendelse
- Administration af brugere af computeren
- Justering af enhedsspecifikke parametre
- Konfiguration af installerede Security Manager-programmer
- Tilføjelse af ekstra Security Manager-programmer

Ved brug af kontrolpanelet til Security Manager kan almindelige brugere udføre følgende opgaver:

- Konfigurere indstillinger, som fås fra en administrator
- Tillade begrænsede kontrolelementer til nogle HP ProtectTools-moduler

De softwaremoduler, der findes til din computer, kan variere afhængigt af din model.

HP ProtectTools-softwaremodulerne kan være forudinstallerede, forudindlæste eller tilgængelige til download fra HP's websted. Besøg http://www.hp.com, hvis du vil vide mere.

BEMÆRK: Oplysningerne i denne brugervejledning er skrevet på det grundlag, at du allerede har installeret de pågældende HP ProtectTools-softwaremoduler.

Funktioner i HP ProtectTools

Følgende tabel viser de vigtigste funktioner i HP ProtectTools-moduler.

Modul	Vigtige funktioner
HP ProtectTools Security Manager Administrative Console (for administratorer)	• Opsætte og konfigurere sikkerhedsniveauer og sikkerhedslogonmetoder ved hjælp af installationsguiden til Security Manager. • Konfigurere indstillinger, som er skjult fra basisbrugere. • Konfigurere Device Access Manager-konfigurationer og brugeradgang. • Tilføje og fjerne HP ProtectTools-brugere og visning af brugerstatus ved hjælp af administratorværktøjer.
HP ProtectTools Security Manager (for almindelige brugere)	• Organisere, vælge og ændre brugernavne og adgangskoder. • Konfigurere og ændre brugerlegitimationsoplysninger, som f.eks. Windows-adgangskode og Smart Card. • Konfigurere og ændre File Sanitizer Shred, Bleaching og Settings. • Få vist indstillinger til Device Access Manager. • Konfigurere indstillingerne Preferences (Præferencer) samt Sikkerhedskopiering og gendannelse.
Credential Manager til HP ProtectTools (Password Manager)	• Gemme, organisere og beskytte dine navne og adgangskoder. • Opsætte logon-skærmbilleder til websteder og programmer for hurtig og sikker adgang. • Gemme brugernavne og adgangskoder til websteder ved at indtaste dem i Password Manager. Næste gang du besøger dette websted, udfylder Password Manager dem automatisk og fremsender oplysningerne. • Oprette mere komplekse adgangskoder for større kontosikkerhed. Password Manager udfylder og fremsender oplysningerne automatisk.
Drive Encryption til HP ProtectTools (kun udvalgte modeller)	• Levere fuldstændig kryptering af hele harddisken. • Gennemtvinge opstartsgodkendelse for at dekryptere og få adgang til dataene.
Privacy Manager til HP ProtectTools (kun udvalgte modeller)	• Anvende avancerede logonteknikker til at verificere kilden, integriteten og sikkerheden ved kommunikation ved anvendelse af e-mail, Microsoft® Office-dokumenter eller onlinemeddelelser.
File Sanitizer til HP ProtectTools	• Makulere digitale aktiver (følsomme oplysninger, herunder applikationsfiler, historisk eller webrelateret indhold eller andre fortrolige data) på computeren og renser jævnligt harddisken.
Device Access Manager til HP ProtectTools (kun udvalgte modeller)	• Gøre det muligt for it-chefer af styre adgang til enheder baseret på brugerprofiler. • Forhindre uautoriserede brugere i at fjerne data ved hjælp af eksterne lagringsmedier og sende virus til systemet fra eksterne medier. • Tillade administratorer at deaktivere adgang til skrivbare enheder for bestemte personer eller brugergrupper.

Opnå vigtige sikkerhedsmål

HP ProtectTools-modulerne kan fungere sammen og give løsninger på forskellige sikkerhedsområder, herunder følgende vigtige sikkerhedsmål:

- Beskyttelse mod målrettet tyveri
- Begrænsning af adgang til følsomme data
- Forhindring af uautoriseret adgang fra interne eller eksterne placeringer
- Oprettelse af effektive adgangskodepolitikker

Beskyttelse mod målrettet tyveri

Et eksempel på målrettet tyveri ville være tyveri af en computer, der indeholder fortrolige data og kundeoplysninger, ved et sikkerhedscheckpoint i en lufthavn. Følgende funktioner er med til at beskytte mod målrettet tyveri:

- Hvis preboot-godkendelsesfunktionen aktiveres, forhindres adgang til operativsystemet. Se fremgangsmåden nedenfor:
  - Security Manager
  - Drive Encryption

Begrænsning af adgang til følsomme data

Forestil dig, at en kontraktkontrollør arbejder onsite og har fået computeradgang til at gennemse følsomme økonomiske data og du ikke ønsker, at kontrolløren kan udskrive filerne eller gemme dem på en skrivbar enhed, f.eks. en cd. Følgende funktion er med til at begrænse adgang til data:

- Device Access Manager til HP ProtectTools giver IT-chefer mulighed for at begrænse adgang til skrivbare enheder, så følsomme oplysninger ikke kan udskrives eller kopieres fra harddisken til flytbare medier.

Forhindring af uautoriseret adgang fra interne eller eksterne placeringer

Uautoriseret adgang til en ikke-sikret virksomheds-pc udgør en meget håndgribelig risiko for firmanetværksressourcer, som f.eks. oplysninger fra finansieringsselskaber, en leder eller et R&D-team, og for private oplysninger, som f.eks. patientjournaler eller personlige, økonomiske optegnelser. Følgende funktioner er med til at forhindre uautoriseret adgang:

- Hvis preboot-godkendelsesfunktionen aktiveres, forhindres adgang til operativsystemet. Se fremgangsmåden nedenfor:
  - Password Manager
  - Drive Encryption
- Password Manager er med til at sikre, at en uautoriseret bruger ikke kan få adgangskoder eller adgang til adgangskodebeskyttede programmer.
- Device Access Manager til HP ProtectTools giver it-chefer mulighed for at begrænse adgang til skrivbare enheder, så følsomme oplysninger ikke kan kopieres fra harddisken.

- Med File Sanitizer kan du sikre sletning af data ved at makulere kritiske filer og mapper eller rense harddisken (ved at overskrive de slettede data, som stadig kan gendannes).
- DriveLock er med til at sikre, at der ikke kan opnås adgang til data, selvom harddisken fjernes og installeres i et ikke-sikret system.

Oprettelse af stærke adgangskodepolitikker

Hvis et mandat træder i kraft, som kræver brug af en stærk adgangskodepolitik til snesevis af webbaserede programmer og databaser, yder Security Manager et beskyttende lager til adgangskoder og Single Sign On-ansvarlighed.

Yderligere sikkerhedselementer

Tildeling af sikkerhedsroller

Ved styring af computersikkerhed (især i store organisationer) er det vigtigste at opdele ansvarsområderne og rettighederne blandt de forskellige typer administratorer og brugere.

BEMÆRK: I en lille organisation eller for enkeltpersoner kan disse roller indehaves af den samme person.

Sikkerhedspligter og -privilegier til HP ProtectTools kan opdeles i følgende roller:

- Sikkerhedschef - Definerer sikkerhedsniveauet for firmaet eller netværket og bestemmer de sikkerhedsfunktioner, der skal implementeres, f.eks. Java™ Cards, biometriske læsere eller USB-tokens.

  BEMÆRK: Mange af funktionerne i HP ProtectTools kan tilpasses af sikkerhedschefen i samarbejde med HP. Yderligere oplysninger finder du på HP's websted på adressen http://www.hp.com.

- Administrator - Angiver og styrer de sikkerhedsfunktioner, der defineres af sikkerhedsmedarbejderen. Kan også aktivere og deaktivere nogle funktioner. Hvis f.eks. sikkerhedsmedarbejderen har besluttet at implementere Java Cards, kan IT-administratoren aktivere BIOS-sikkerhedstilstand for Java Cards.

- Bruger - Bruger sikkerhedsfunktionerne. Hvis sikkerhedschefen og IT-administratoren f.eks. har aktiveret Java Cards til systemet, kan brugeren definere PIN-koden til Java Cards og bruge kortet til godkendelse.

FORSIGTIG: Administratorer opfordres til at følge "bedste praksis" ved begrænsning af privilegier til slutbrugere og begrænsning af brugeradgang.

Der bør ikke gives administrative privilegier til uautoriserede brugere.

Styring af adgangskoder til HP ProtectTools

De fleste funktioner i HP ProtectTools Security Manager er sikrede af adgangskoder. Følgende tabel viser de almindeligt brugte adgangskoder, det softwaremodul, hvor adgangskoden defineres, og adgangskodens funktion.

Adgangskoder, der kun defineres og bruges af IT-administratorer, er også angivet i tabellen. Alle andre adgangskoder kan være defineret af almindelige brugere eller administratorer.

Adgangskode til HP ProtectTools	Angiv i følgende modul	Funktion
Adgangskode til Windows-logon	Windows® kontrolpanel eller HP ProtectTools Security Manager	Kan anvendes til manuelt logon og til godkendelse til adgang til forskellige funktioner i Security Manager.
Adgangskoder til sikkerhedskopiering og gendannelse i Security Manager	Security Manager, af individuel bruger	Beskytter adgangen til sikkerhedskopi- og gendannelsesfil for Security Manager.
Java™ Card-PIN	Java Card-sikkerhed	Beskytter adgangen til Java Card-indhold og godkender brugerne af Java Card. Når det bruges til godkendelse ved start, beskytter Java Card-PIN-koden også adgangen til

Adgangskode til HP ProtectTools	Angiv i følgende modul	Funktion
		hjælpeprogrammet Computer Setup (Computeropsætning) og computerens indhold. Godkender brugere af Drive Encryption, hvis Java Card-tokenet vælges.

Oprettelse af en sikker adgangskode

Når du opretter adgangskoder, skal du først følge eventuelle specifikationer, der defineres af programmet. Du bør dog overveje følgende retningslinjer som en hjælp til at oprette stærke adgangskoder og reducere risikoen for, at din adgangskode bliver opdaget:

- Brug adgangskoder med mere end seks tegn. Helst mere end otte.
- Bland store og små bogstaver i hele adgangskoden.
- Når det er muligt, skal du blande alfanumeriske tegn og inkludere specialtegn og tegnsætningstegn.
- Udskift specialtegn eller tal med bogstaver i et nøgleord. Du kan f.eks. bruge tallet 1 i stedet for bogstaverne I eller L.
- Kombiner ord fra to eller flere sprog.
- Opdel et ord eller en sætning med tal eller specialtegn i midten, f.eks. “Mary2-2Cat45”.
- Brug ikke en adgangskode, der kan findes i en ordbog.
- Brug ikke dit navn som adgangskode eller andre personlige oplysninger, f.eks. fødselsdato, dit kæledyrs navn eller mors pigenavn, selv om du staver det bagfra.
- Skift adgangskoder regelmæssigt. Måske skal du blot ændre et par tegn for at forandre tingene.
- Hvis du skriver din adgangskode ned, må du ikke gemme den et synligt sted tæt på computeren.
- Gem ikke adgangskoden i en fil, f.eks. en e-mail, på computeren.
- Del ikke konti med eller fortæl nogen om din adgangskode.

Sikkerhedskopiering og gendannelse af HP ProtectTools-legitimationsoplysninger

Du kan anvende funktionerne til sikkerhedskopiering og gendannelse i HP ProtectTools til at vælge og sikkerhedskopiere data og indstillinger for HP ProtectTools-legitimationsoplysninger.

2 Sådan kommer du igang med opsætningsguiden

Guiden Installation til HP ProtectTools fører dig gennem opsætning af de mest almindelige anvendte funktioner i Security Manager. Der er imidlertid en masse ekstra funktioner tilgængelige via HP ProtectTools Administrative Console. De samme indstillinger, der findes i guiden samt ekstra sikkerhedsfunktioner kan konfigureres via konsollen, som der er adgang til fra Start-menuen i Windows®. Disse indstillinger gælder for computeren og alle de brugere, der deler computeren.

1. Når du logger op efter en uge med den første opsætning af computeren, eller når en bruger med administrative rettigheder for første gang fører en finger hen over fingeraftrykslæseren, starter guiden til installation af Security Manager automatisk for at hjælpe dig igennem de grundlæggende trin i konfiguration af programmet. En selvstudievideo vedr. opsætning af computeren starter automatisk.

   - eller -

   Åbn HP ProtectTools Security Manager fra ikonet **Gadget** (Gadget) i sidebjælken til Windows eller på proceslinjen i meddelelsesområdet yderst til højre for proceslinjen.

   

   Farven på den øverste linje af ikonet Gadget angiver en af følgende tilstande:

   - Rød - HP ProtectTools er ikke installeret, eller der er opstået en fejltilstand i en af ProtectTools-modulerne.
   - Gul - Kontroller siden Applications Status (Programstatus) i Security Manager for ændring af indstillinger.
   - Blå - HP ProtectTools er installeret og fungerer korrekt.

   BEMÆRK: Ikonet Gadget er ikke tilgængelig i Windows XP.

   - eller -

Klik på **Start**, klik på **Alle programmer**, og klik derefter på **HP ProtectTools Administrative Console**.

2. Læs skærmbilledet “Velkommen”, og klik derefter på **Next** (Næste).

BEMÆRK: På velkomstskærmen kan du deaktivere yderligere visning af guiden ved at vælge én af funktionerne.

3. Installationsguiden spørger dig, om du vil verificere din identitet.

   Indtast din Windows-adgangskode, eller scan dine fingeraftryk ved hjælp af fingeraftrykslæseren, og klik derefter på **Næste**.

   Hvis hverken en fingeraftrykslæser eller et chipkort er tilgængeligt, vil du blive bedt om at indtaste din Windows-adgangskode. Du skal bruge denne adgangskode fremover, når der kræves godkendelse.

   Hvis du endnu ikke har oprettet en Windows-adgangskode, bliver du bedt om at oprette en. For at kunne beskytte din Windows-konto mod adgang fra uautoriserede personer samt for at bruge HP ProtectTools Security Manager-funktionerne, kræves en Windows-adgangskode.

4. Installationsguiden hjælper dig gennem processen med indstilling af sikkerhedsfunktioner, der gælder for alle brugere af computeren:

   - Windows Logon Security beskytter dine Windows-konti ved at kræve brugen af specifikke legitimationsoplysninger for at få adgang.
   - Drive Encryption beskytter dine data ved at kryptere dine harddiske, hvilket gør oplysningerne ulæsbare for dem uden korrekt tilladelse.
   - Pre-Boot Security beskytter din computer ved at forhindre adgang fra uautoriserede personer før start af Windows.

     BEMÆRK: Pre-Boot Security er ikke tilgængelig, hvis din computer BIOS ikke understøtter det.

   Marker dets afkrydsningsfelt for at aktivere en sikkerhedsfunktion. Jo flere funktioner, du vælger, des mere sikker bliver din computer.

5. På guidens sidste side skal du klikke **Finish** (Udfør).

   Kontrolpanelet til Security Manager vises.

BEMÆRK: Hvis du ikke fuldfører guiden, starter den automatisk to gange mere. Efter dette kan du få adgang til guiden fra meddelelsesboblen, der vises i meddelelsesområdet længst til højre på proceslinjen (medmindre du har deaktiveret den, indtil opsætningen er færdiggjort.

3 HP ProtectTools Security Manager Administrative Console

Administration af HP ProtectTools Security Manager sker via Administrative Console.

BEMÆRK: Administration af HP ProtectTools kræver administratorrettigheder.

Konsollen tilbyder følgende funktioner:

- Aktivering eller deaktivering af sikkerhedsfunktioner
- Administration af brugere af computeren
- Justering af enhedsspecifikke parametre
- Konfiguration af Security Manager-programmer
- Tilføjelse af ekstra Security Manager-programmer

▲ Hvis du vil bruge programmerne i HP ProtectTools Security Manager, skal du starte HP ProtectTools Security Manager fra Start-menuen eller højreklikke på Security Manager-ikonet i meddelelsesområdet, der findes yderst til højre på proceslinjen.

HP ProtectTools Administrative Console og dets programmer er tilgængelige for alle brugere, der deler denne computer.

Åbning af Administrative Console

Ved administrative opgaver, som f.eks. opsætning af systempolitikker eller konfiguration af software, skal du åbne konsollen på følgende måde:

- Klik på **Start**, klik på **Alle programmer**, klik på **HP** og klik derefter på **HP ProtectTools Administrative Console**.

  - eller -

  Klik på **Administration** i venstre rude i kontrolpanelet i Security Manager.

Vedr. brugeropgaver, som f.eks. registrering af fingeraftryk eller ved brug af Security Manager, skal du åbne konsollen på følgende måde:

- Klik på **Start**, klik på **Alle programmer**, klik på **HP** og klik derefter på **HP ProtectTools Security Manager**.

  - eller -

  Dobbeltklik på ikonet for **HP ProtectTools Security Manager** i meddelelsesområdet yderst til højre på proceslinjen.

Brug af Administrative Console

Security Manager Administrative Console er den centrale placering for administration af HP ProtectTools Security Manager.

Konsollen består af følgende komponenter:

- **Værktøjer** - Viser følgende kategorier til konfiguration af sikkerhed på din computer:
  - **Start** - Giver mulighed for at vælge de sikkerhedsopgaver, der skal udføres.
  - **System** - Giver mulighed for at konfigurere sikkerhedsfunktioner og at godkende brugere og enheder.
  - **Programmer** - Viser generelle indstillinger til HP ProtectTools Security Manager- og til Security Manager-programmer.
  - **Data** - Giver en udvidet menu med links til Security Manager-programmer, der beskytter dine data.
- **Management Tools** (Administrationsværktøjer) – Giver oplysninger om ekstra værktøjer. Panelet viser følgende valg:
  - **HP ProtectTools Security Manager Setup Wizard** (Installationsguiden til HP ProtectTools Security Manager)– fører dig gennem opsætning af HP ProtectTools Security Manager.
  - **Help** (Hjælp) – Viser denne Hjælp-fil, der giver oplysninger om Security Manager og dets forudinstallerede programmer. Hjælp til programmer, som du kan tilføje, findes i disse programmer.
  - **About** (Om) – Viser oplysninger om HP ProtectTools Security Manager, som f.eks. versionsnummeret og oplysninger om copyright.
- **Main area** (Hovedområde) – Viser programspecifikke skærmbilleder.

4 Konfiguration af dit system

Der er adgang til systemgruppen fra menupanelet til værktøjer på venstre side af skærmbilledet HP ProtectTools Administrative Console. Du kan bruge programmerne i denne gruppe til at administrere politikker og indstillinger til computeren, dens brugere og enheder.

Følgende programmer er inkluderet i systemgruppen:

- **Security** (Sikkerhed) - Håndterer funktioner, godkendelse og indstillinger, der styrer, hvordan brugere anvender denne computer.
- **Users** (Brugere) - Installerer, administrerer og registrerer brugere af denne computer.
- **Devices** (Enheder) - Administrerer indstillinger til sikkerhedsenheder, der er indbygget eller sluttet til computeren.

Installation af godkendelse til denne computer

Med programmet Authentication kan du vælge, hvilke sikkerhedsfunktioner der bør implementeres på denne computer, angive politikker, der styrer adgang til computeren samt konfigurere yderligere avancerede indstillinger. Du kan angive de legitimationsoplysninger, der kræves for at godkende hver brugerklasse, når du logger på Windows eller logger ind på websteder og programmer under en brugersession.

Sådan opsætter du godkendelse på din computer:

1. Klik på **Authentification** (Godkendelse) i menupanelet til sikkerhed.
2. Hvis du vil konfigurere logongodkendelse, skal du klikke på fanen **Logonpolitik**, foretage ændringer og klikke på **Anvend**.
3. Hvis du vil konfigurere session-godkendelse, skal du klikke på fanen **Session Policy** (Session-politik), foretage ændringer og klikke på **Anvend**.

Logonpolitik

Hvis du vil definere politikker, der styrer de legitimationsoplysninger, der kræves for at godkende en bruger, når denne logger på Windows:

1. Klik på **Sikkerhed**, og klik derefter på **Godkendelse** i menuen Værktøjer.
2. Klik på en brugerkategori på fanen **Logonpolitik**.
3. Angiv de godkendelsesoplysninger, der kræves til den valgte brugerkategori. Du skal angive mindst ét kreditiv.
4. Vælg om ENHVER (kun én) af de angivne legitimationsoplysninger er påkrævet, eller om ALLE de angivne legitimationsoplysninger er påkrævet for at godkende en bruger. Du kan også forhindre enhver bruger i at få adgang til computeren.
5. Klik på **Anvend**.

Session Policy (Session-politik)

Sådan definerer du de politikker, der styrer de legitimationsoplysninger, der kræves for at få adgang til programmerne i HP ProtectTools under en Windows-session:

1. Klik på **Sikkerhed**, og klik derefter på **Godkendelse** i menuen Værktøjer.
2. Klik på en brugerkategori på fanen **Sessionspolitik**.
3. Angiv de godkendelsesoplysninger, der kræves til den valgte brugerkategori.
4. Vælg om ÉN af de angivne legitimationsoplysninger er påkrævet, eller om ALLE de angivne legitimationsoplysninger er påkrævet for at godkende en bruger. Du kan også kræve ingen godkendelse for at få adgang til HP ProtectTools-softwaren.
5. Klik på **Anvend**.

Indstillinger

Du kan tillade en eller flere af følgende sikkerhedsindstillinger:

- **Allow One Step logon** (Tillad ét trins logon) - Giver brugere af denne computer mulighed for at springe Windows-logon over, hvis godkendelsen blev udført på BIOS eller krypteret diskniveau.
- **Allow HP SpareKey authentication for Windows logon** (Tillad HP SpareKey-godkendelse ved Windows-logon) - Giver brugere af denne computer mulighed for at bruge HP SpareKey-funktionen til at logge på Windows, uanset enhver anden godkendelsespolitik, der kræves af Security Manager.

Sådan redigerer du indstillingerne:

1. Klik for at aktivere eller deaktivere en specifik indstilling.
2. Klik på **Anvend** for at gemme de ændringer, du har foretaget.

Administration af brugere

I programmet Users kan du overvåge og administrere denne computers brugere af HP ProtectTools.

Alle brugere af HP ProtectTools vises og verificeres op mod de politikker, der er angivet via Security Manager, og om de har eller ikke har registreret de relevante legitimationsoplysninger, der giver dem mulighed for at opfylde disse politikker.

Vælg blandt følgende indstillinger for at administrere brugere:

- Klik på **Tilføj** for at føje yderligere brugere til.
- Klik på en bruger, og klik derefter på **Slet** for at slette en bruger.
- Klik på brugeren, og klik derefter på **Enroll** (Registrer) for at registrere fingeraftryk eller opsætte yderligere legitimationsoplysninger for brugeren.
- For at vise politikkerne for en specifik bruger skal du vælge brugeren og vise politikkerne i det nederste vindue.

Angivelse af enhedsindstillinger

I programmet Device kan du angive indstillinger, som er tilgængelige for alle indbyggede eller tilsluttede sikkerhedsenheder, der genkendes af HP ProtectTools Security Manager.

Fingeraftryk

Siden Fingerprints (Fingeraftryk) har tre faner: Enrollment (Registrering), Sensitivity (Følsomhed) og Advanced (Avanceret).

Registrering

Du kan vælge minimums- og maksimumsantallet af fingeraftryk, som en bruger må registrere.

Du kan også fjerne alle dataene fra fingeraftrykslæseren.

△ **FORSIGTIG:** Sletning af alle dataene fra fingeraftrykslæseren sletter alle fingeraftryksdata for alle brugere, inkl. administratorer. Hvis logonpolitikken kun kræver fingeraftryk, kan alle brugere blive forhindret i at logge på computeren.

Følsomhed

Hvis du vil justere den følsomhed, der anvendes af fingeraftrykslæseren, når den scanner dine fingeraftryk, skal du flytte skyderen.

Hvis dit fingeraftryk afvises hele tiden, kan en lavere følsomhed være nødvendig. En højere indstilling forøger følsomheden for at variere fingeraftrykksscanninger og reducerer muligheden for en falsk accept. Indstillingen Medium-High (Medium-Høj) giver et godt miks af sikkerhed og ansvarlighed.

Avanceret

Du kan konfigurere fingeraftrykslæseren til at spare strøm, når computeren kører på batteristrøm.

Smart Card (chipkort)

Du kan konfigurere computeren til automatisk at låse, når et chipkort fjernes. Computeren låser imidlertid kun, hvis chipkortet blev brugt som en godkendelsesoplysning, når der logges på Windows. Fjernelse af et chipkort, der ikke blev anvendt til at logge på Windows, låser ikke computeren.

▲ Markér afkrydsningsfeltet for at aktivere eller deaktivere låsning af computeren, når chipkortet fjernes.

Ansigt

Du kan indstille sikkerhedsniveauet for ansigtsgenkendelse til at balancere mellem brugervenlighed og sværhedsgraden for at bryde computerens sikkerhed.

1. Klik på **Start**, klik på **Alle programmer**, klik på **HP** og klik derefter på **HP ProtectTools Administrative Console**.
2. Klik på **Enheder**, og klik derefter på **Face** (Ansigt).

3. For mere anvendelighed: Klik på skyderen, og flyt den til venstre eller for større nøjagtighed: Klik på skyderen, og flyt den til højre.

   - **Convenience** (Anvendelighed) – For at gøre det nemmere for registrerede brugere at få adgang i marginale situationer: Klik på skyderen for at flytte den til positionen **Convenience** (Anvendelighed).
   - **Balance** (Balance) – For at give et godt kompromis mellem sikkerhed og brugervenlighed, hvis du har følsomme informationer, eller hvis din computer er placeret et sted, hvor der kan forekomme forsøg på uautoriseret logon: Klik på skyderen for at flytte den til stillingen **Balance** (Balance).
   - **Accuracy** (Nøjagtighed) – For at gøre det sværere for en bruger at få adgang, hvis de registrerede motiver eller de aktuelle lysforhold er under det normale, og det er mindre sandsynligt, at en falsk accept kan forekomme: Klik på skyderen for at flytte den til stillingen **Accuracy** (Nøjagtighed).

BEMÆRK: Sikkerhedsniveauet gælder for alle brugere

4. Klik på **Apply** (Anvend).

Avancerede indstillinger

1. Klik på **Start**, klik på **Alle programmer**, klik på **HP** og klik derefter på **HP ProtectTools Administrative Console**.
2. Klik på **Enheder**, og klik derefter på **Face** (Ansigt).
3. Klik på **Advanced** (Avanceret).
   - **Do not require user name for Windows logon** (Kræv ikke et brugernavn til Windows-logon).
     - Vælg afkrydsningsfeltet for at gøre det muligt at logge på Windows uden et brugernavn.
     - Ryd afkrydsningsfeltet for at kræve et brugernavn ved logon.
   - **Enforce the use of PIN for face logon** (Kræv brug af PIN-kode ved ansigtslogon) – Vælg afkrydsningsfeltet for at kræve, at hver bruger indstiller og bruger en PIN-kode ved for logon.
     - **Minimum length allowed for PIN** (Mindste tilladte længde for PIN-kode) – Klik på pil op for at forøge det mindste antal tegn, der kræves for en PIN-kode.
     - **Maximum length allowed for PIN** (Største tilladte længde for PIN-kode) – Klik på pil ned for at formindske det højeste antal tegn, der kræves for en PIN-kode.
     - **Maximum retries allowed for PIN** (Største antal forsøg med PIN-kode) – klik på pil op for at formindske det højeste antal gange, PIN-koden kan genindtastes.
4. Klik på **OK**.

5 Konfiguration af dine programmer

Der er adgang til programgruppen fra menupanelet til sikkerhedsprogrammer til venstre for HP ProtectTools Administrative Console. Du kan anvende Indstillinger for at tilpasse adfærden af de aktuelt installerede HP ProtectTools Security Manager-programmer.

Sådan redigerer du programindstillingerne:

1. Klik på **Indstillinger** i menuen Værktøjer i gruppen **Programmer**.
2. Klik for at aktivere eller deaktivere en specifik indstilling.
3. Klik på **Anvend** for at gemme de ændringer, du har foretaget.

Fanen Generelt

Følgende indstillinger er tilgængelige på fanen Generelt:

- **Do not automatically launch the Setup Wizard for administrators** (Start ikke automatisk guiden Installation for administratorer) - Vælg denne indstilling for at forhindre guiden i automatisk at åbne ved logon.
- **Do not automatically launch the Getting Started wizard for users** – (Start ikke automatisk guiden Sådan kommer du i gang for brugere) - Vælg denne indstilling for at forhindre brugerindstilling i automatisk at åbne ved logon.

Fanen Programmer

De indstillinger, der vises her, ændres muligvis, når der føjes nye programmer til Security Manager. De minimale indstillinger, der vises som standard, er følgende:

- **Applications status** (Programstatus) – Gør det muligt at vise status for alle programmer.
- **Security Manager** (Security Manager) – Aktiverer programmet Password Manager for alle brugere af computeren.
- **Privacy Manager** (Privacy Manager) – Aktiverer programmet Privacy Manager for alle brugere af computeren.
- **Enable the Discover more button** (Aktiver knappen Se mere) – Giver alle brugerne at denne computer mulighed for at føje programmer til HP ProtectTools Security Manager ved at klikke på knappen **[+] Discover more** (Se mere).

Klik på knappen **Restore Defaults** (Gendan standardindstillinger), hvis alle programmer skal vende tilbage til deres standardindstillinger.

6 Administrationsværktøjer

Der kan være flere programmer tilgængelige for tilføjelse af administrationsværktøjer til Security Manager. Administratoren af denne computer kan deaktivere denne funktion via programmet Settings (Indstillinger).

Klik på **[+] Administrationsværktøjer** for at tilføje flere administrationsværktøjer.

Opdateringer og meddelelser

Hvis der er en internetforbindelse til rådighed, kan du få adgang til webstedet DigitalPersona http://www.digitalpersona.com/ for at søge efter nye programmer eller installere en tidsplan for automatiske opdateringer.

1. Marker afkrydsningsfeltet **Keep me informed about new applications and updates** (Hold mig informeret om nye programmer og opdateringer) for at anmode om information om nye programmer og opdateringer.
2. Vælg antallet af dage for at opsætte en plan over automatiske opdateringer.
3. Klik på **Kontroller nu** for at kontrollere, om der er kommet opdateringer.

7 HP ProtectTools Security Manager

HP ProtectTools Security Manager giver dig mulighed for at øge sikkerheden for din computer væsentligt.

Du kan bruge forudindlæste Security Manager-programmer samt de ekstra programmer, der er tilgængelige for øjeblikkelig download fra internettet:

- Administrere logon og adgangskoder
- Nemt ændre din adgangskode til Windows®-operativsystemet
- Angive programpræferencer
- Anvende fingeraftryk til ekstra sikkerhed og ansvarlighed
- Registrer et eller flere motiver til ansigtsgenkendelse
- Installere et chipkort for godkendelse
- Sikkerhedskopiere og gendanne dine programdata
- Samt flere programmer

Åbning af HP ProtectTools Security Manager

Du kan åbne HP ProtectTools Security Manager på en af følgende måder:

- Klik på **Start**, klik på **Alle programmer**, klik på **HP** og klik derefter på **HP ProtectTools Security Manager**.
- Dobbeltklik på ikonet for **HP ProtectTools** i meddelelsesområdet yderst til højre på proceslinjen.
- Højreklik på ikonet for **HP ProtectTools**, og klik på **Open HP ProtectTools Security Manager** (Åbn HP ProtectTools Security Manager).
- Klik på gadget **Security Manager ID Card** (Id-kort til Security Manager) på sidebjælken i Windows.
- Tryk på hot key-kombinationen ctrl+Windows+h for at åbne menuen Security Manager Quick Links (Hurtige link).

Brug af kontrolpanelet til Security Manager

Kontrolpanelet til Security Manager er det centrale sted for nem adgang til Security Manager-funktioner, programmer og indstillinger.

▲ Klik på **Start**, klik på **Alle programmer**, klik på **HP**, og klik derefter på **HP ProtectTools Security Manager** for at åbne kontrolpanelet til Security Manager.

Kontrolpanelet består af følgende komponenter:

- **ID Card** (Id-kort) – Viser brugernavnet til Windows og et valgt billede, der bekræfter den brugerkonto, der er logget på.
- **Security Applications** (Sikkerhedsprogrammer) – Viser en udvidet menu med links til konfiguration af følgende sikkerhedskategorier:
  - **Credential Manager**
  - **My Data (Mine data)**
- **Discover more** (Se mere) – Åbner en side, hvor du kan finde flere programmer til at forbedre sikkerheden for din identitet, dine data og din kommunikation.
- **Main area** (Hovedområde) – Viser programspecifikke skærmbilleder.
- **Administration** (Administration) – Åbner HP ProtectTools Administrative Console.
- **Hjælp-knap** – Viser oplysninger om det aktuelle skærmbillede.
- **Advanced** (Avanceret) – Giver mulighed for adgang til følgende funktioner:
  - **Preferences** (Præferencer) – Giver mulighed for at personliggøre indstillingerne til Security Manager.
  - **Backup and Restore** (Sikkerhedskopiering og gendannelse) – Giver mulighed for at sikkerhedskopiere eller gendanne data.
  - **About** (Om) – Viser versionsoplysninger om Security Manager.

Opsætningsprocedurer

Registrering af legitimationsoplysninger

Du kan bruge siden Min identitet til at registrere dine forskellige godkendelsesmetoder eller legitimationsoplysninger. Når de er registreret, kan du bruge disse metoder til at logge på Security Manager.

Registrering af dine fingeraftryk

Hvis din computer har en fingeraftrykslæser indbygget eller tilsluttet, hjælper installationsguiden til HP ProtectTools Security Manager dig gennem processen med opsætning eller "registrering" af dine fingeraftryk.

1. Et omrids af to hænder vises. De fingre, der allerede er registreret, fremhæves med grøn. Klik med en finger på omridset.

   BEMÆRK: Hvis du vil slette et tidligere registreret fingeraftryk, skal du klikke på dets finger.

2. Når du har valgt den finger, du vil registrere, bliver du bedt om at scanne fingeren, indtil dens fingeraftryk er registreret korrekt. En registreret finger fremhæves med grøn på omridset.

3. Du skal registrere mindst to fingre, pegefinger eller langfinger foretrækkes. Gentag trin 1 til 3 for den anden finger.

4. Klik på **Next** (Næste), og følg derefter anvisningerne på skærmen.

BEMÆRK: Når fingeraftryk registreres via Sådan kommer du i gang-processen, gemmes oplysningerne om fingeraftryk ikke, før du klikker på **Next** (Næste). Hvis du lader computeren være inaktiv i et stykke tid eller lukker programmet, gemmes de ændringer, du foretog, **ikke**.

Registrering af motiver

Du skal registrere et eller flere motiver for at kunne anvende ansigtslogon.

Sådan registreres et nyt motiv via installationsguiden til HP ProtectTools Security Manager:

1. Klik på ikonet **HP ProtectTools Security Manager** i panelet til højre på skærmen.

2. Angiv din Windows®-adgangskode, og klik derefter på **Next** (Næste).

3. Under **Enable security features** (Aktiver sikkerhedsfunktioner) skal du vælge afkrydsningsfeltet **Windows Logon Security** og derefter klikke på **Next** (Næste).

4. Under **Choose your credentials** (Vælg dine legitimationsoplysninger) skal du vælge afkrydsningsfeltet **Face** (Ansigt) og derefter klikke på **Next** (Næste).

5. Klik på **Enroll a new scene** (Tilmeld en ny scene).

Når du har registreret korrekt, kan du også registrere et nyt motiv, hvis du har oplevet problemer med logon, fordi en eller flere af følgende betingelser er ændret:

- Din ansigt er ændret betydeligt, siden din sidste registrering.
- Lysforholdene er helt anderledes end ved de tidligere registreringer.
- Du brugte (ikke) briller ved din seneste registrering.

BEMÆRK: Hvis du har problemer med at optage scener, kan du prøve at gå tættere på webkameraet. Ligesom med alle andre typer fotografering eller videooptagelse, er lys og kontrast utrolig vigtigt. Sørg for, at lyset i din session hovedsagelig er i forgrunden i stedet for i baggrunden. Hvis du ikke synes at Face Recognition (Ansigtsgenkendelse) genkender dig hurtigt, kan du eventuelt genoptage din scene med forbedrede lysforhold.

Sådan registreres et nyt motiv via HP ProtectTools Security Manager:

1. Klik på **Start**, klik på **Alle programmer**, klik på **HP** og klik derefter på **HP ProtectTools Security Manager**.
2. Klik på **Credentials** (Legitimationsoplysninger), og klik derefter på **Face** (Ansigt).
3. Klik på **Enroll a new scene** (Tilmeld en ny scene).

Avancerede brugerindstillinger

1. Klik på **Start**, klik på **Alle programmer**, og klik derefter på **HP ProtectTools Security Manager**.
2. Klik på **Set up your authentication credentials** (Angiv dine godkendelsesoplysninger), og klik derefter på **Face** (Ansigt).
3. Klik på knappen **Avanceret**, og vælg derefter blandt følgende muligheder.

   a. For at kræve brug af en PIN-kode ved ansigtslogon: Klik på **Create PIN** (Opret PIN-kode), indtast din Windows-adgangskode, indtast den nye PIN-kode, og bekræft derefter den nye PIN-kode ved at skrive den igen.

   b. Vælg efter ønske yderligere indstillinger. Disse indstillinger gælder kun for den aktuelle bruger:

   - **Play sound on face recognition events (Afspil lyd ved ansigtsgenkendelse)**
     - Vælg afkrydsningsfeltet for at afspille lyd, når ansigtsgenkendelse lykkes eller mislykkes.
     - Ryd afkrydsningsfeltet for at deaktivere denne mulighed.
   - **Prompt to update scenes when logon fails (Spørg om opdatering af motiver, når logon mislykkes)**
     - Vælg afkrydsningsfeltet for at gøre det muligt for brugeren at opdatere motiver, hvis ansigtslogon mislykkes. Hvis verificeringen når “måske-tærsklen”, bliver brugeren bedt om at beslutte, om der skal indsættes det levende billede i det “mislykkede” logon som det aktuelle motiv for at forøge chancen for korrekt logon næste gang.
     - Ryd afkrydsningsfeltet for at deaktivere denne mulighed.
   - **Prompt to enroll a new scene when logon fails (Spørg om at registrere et nyt motiv, når logon mislykkes)**
     - Vælg afkrydsningsfeltet for at vise en meddelelse, der beder brugeren om at registrere et nyt motiv, hvis ansigtslogon mislykkes, og verificeringen ikke når “måske-tærsklen”. Dette kan forøge chancen for korrekt logon næste gang.
     - Ryd afkrydsningsfeltet for at deaktivere denne mulighed.

   c. For at registrere et nyt motiv: Klik på **Enroll a new scene** (Registrer et nyt motiv), og følg derefter instruktionerne på skærmen.

Ændring af din Windows-adgangskode

Security Manager gør ændring af din Windows-adgangskode enklere og hurtigere, end af gøre det via kontrolpanelet i Windows.

Sådan ændrer du Windows-adgangskoden:

1. Klik på **Credentials** (Legitimationsoplysninger), og klik derefter på **Password** (Adgangskode) på kontrolpanelet til Security Manager.
2. Indtast din aktuelle adgangskode i tekstboksen **Current Windows password** (Aktuel Windows-adgangskode).
3. Indtast en ny adgangskode i tekstboksen **New Windows password** (Ny Windows-adgangskode), og indtast den derefter igen i tekstboksen **Confirm new password** (Bekræft ny adgangskode).
4. Klik på **Change** (Skift) for straks at ændre din aktuelle adgangskode til den nye, du har indtastet.

Installation af et chipkort

Hvis du vælger logon med chipkort, og hvis der er indbygget eller tilsluttet en chipkortlæser til din computer, vil installationsguiden til Security Manager bede dig om at installere en personlig chipkort-PIN-kode (personligt identifikationsnummer).

Sådan installerer du chipkortets PIN-kode:

1. Under **Set up smart card** (Installer chipkort) skal du indtaste og bekræfte en PIN-kode.

   Du kan også ændre din PIN-kode. Indtast din nuværende PIN-kode, og indtast derefter en ny.
2. Klik på **Next** (Næste), og følg derefter anvisningerne på skærmen for at fortsætte.

- eller -

▲ Klik på **Credentials** (Legitimationsoplysninger), og klik derefter på **Smart Card** (Chipkort) på kontrolpanelet til Security Manager.

- Sådan installeres en PIN-kode til et chipkort – Skriv og bekræft en PIN-kode under **Set up smart card** (Opsætning af chipkort).
- Sådan ændres din PIN-kode – Indtast først din aktuelle PIN-kode, og indtast og bekræft derefter en ny.

Generelle opgaver

Programmerne i denne gruppe hjælper dig med at administrere forskellige aspekter af din digitale identitet.

- **Security Manager** - Opretter og administrerer Quick Links (Hurtige link), så du har mulighed for at starte og logge på websteder og programmer ved godkendelse af din Windows-adgangskode, dit fingeraftryk eller et chipkort.
- **Legitimationsoplysninger** - Indeholder en måde til nemt at ændre din Windows-adgangskode, registrere dine fingeraftryk eller installere et chipkort.

Klik på knappen [+] **Se mere** i kontrolpanelets nederste venstre hjørne for at tilføje flere programmer. Denne knap kan deaktiveres af administratoren.

Password Manager

Det er nemmere og mere sikkert, når du logger på Windows, websteder og programmer, hvis du anvender Password Manager. Du kan anvende den til at oprette stærkere adgangskoder, så du ikke behøver at skrive det ned eller huske det, og derefter logge på nemt og hurtigt med et fingeraftryk, chipkort eller din Windows-adgangskode.

Password Manager understøtter følgende muligheder:

- Tilføj, rediger eller slet logon fra fanen Manage (Administrer).
- Brug Quick Links (Hurtige link) for at starte din standard browser og logge på ethvert websted eller program, når det er installeret.
- Træk og slip for at organisere dine Quick Links (Hurtige link) til kategorier.
- Se i korte træk om nogle af dine adgangskoder er en sikkerhedsrisiko og automatisk genererer en kompleks stærk adgangskode til brug ved nye websteder.

Mange Password Manager-funktioner er også tilgængelige fra ikonet for Password Manager, der vises, når en webside eller et program-logonskærmbillede har fokus. Klik på ikonet for at få vist en kontekstmenu, hvor du kan vælge mellem følgende funktioner.

For websider eller programmer, hvor der endnu ikke er oprettet en logon

Følgende funktioner vises på kontekstmenuen:

- **Add [somedomain.com] to the Password Manager** (Tilføj [somedomain.com] til Password Manager) - Giver mulighed for at føje en logon til det aktuelle logonskærmbillede.
- **Open Password Manager** (Åbn Password Manager) - Starter Password Manager.
- **Icon settings** (Ikonindstillinger) - Giver mulighed for at angive tilstande, hvor ikonet for Password Manager vises.
- **Help** (Hjælp) - Viser softwarehjælp til Password Manager.

For websider eller programmer, hvor der allerede er oprettet en logon

Følgende funktioner vises på kontekstmenuen:

- **Fill in logon data** (Udfyld logondata) - Anbringer logondata i logonfelter og sender derefter siden (hvis afsendelse blev angivet, hvor logon blev oprettet eller sidst redigeret).
- **Edit logon** (Rediger logon) - Giver mulighed for at redigere dine logondata for dette websted.
- **Add a New Account** (Tilføj en ny konto) - Giver mulighed for at føje en konto til en logon.
- **Open Password Manager** (Åbn Password Manager) - Starter Password Manager-programmet.
- **Help** (Hjælp) - Viser softwarehjælp til Password Manager.

BEMÆRK: Administratoren af denne computer skal have installeret Security Manager for at få mere end én legitimationsoplysning ved verificering af din identitet.

Tilføjelse af logonindstillinger

Du kan nemt tilføje en logon for et websted eller et program ved at indtaste logonoplysningerne én gang. Derefter angiver Password Manager automatisk oplysningerne for dig. Du kan bruge disse logonindstillinger, når du vil gennemse webstedet eller programmet, eller klikke på logon fra menuen **Logons** for at få Password Manager til at åbne webstedet eller programmet og logge dig på.

Sådan tilføjer du en logon:

1. Åbn logonskærmbilledet for et websted eller program.
2. Klik på pilen på ikonet for **Password Manager**, og klik derefter én gang på følgende, afhængigt af om logonskærmbilledet er til et websted eller et program:
   - Klik på **Add [domain name] to Password Manager** (Tilføj [domænenavn] til Password Manager) for et websted.
   - Klik på **Add this logon screen to Password Manager** (Tilføj dette logonskærmbillede til Password Manager) for et program.
3. Indtast dine logondata. Logonfelter på skærmbilledet, og de tilsvarende felter i dialogboksen, identificeres vha. en fed orange kant. Du kan også få vist dialogboksen ved at klikke på **Add Logon** (Tilføj logon) under fanen **Password Manager Manage** (Administrer Password Manager). Nogle funktioner afhænger af de sikkerhedsenheder, der er tilsluttet computeren, f.eks. brug af hot key-kombinationen ctrl+Windows+h, scanning af dit fingeraftryk eller isætning af et chipkort.
   a. For at udfylde et logonfelt med et af de præformaterede valg, skal du klikke på pilene til højre for feltet.
   b. For at få vist adgangskoden for denne logon, skal du klikke på **Show password** (Vis adgangskode).
   c. For at få logonfelterne udfyldt, men ikke afsendt, skal du fjerne markeringen fra afkrydsningsfeltet **Automatically submit logon data** (Send logondata automatisk).
   d. Klik på **OK**, og klik på den godkendelsesmetode, du vil anvende: **Fingerprints** (Fingeraftryk), **Password** (Adgangskode) eller **Face** (Ansigt), og log derefter på med den valgte godkendelsesmetode.

Plustegnet fjernes fra ikonet for Password Manager for at give dig besked om, at der er oprettet logon.

e. Hvis Password Manager ikke detekterer logonfelterne: Klik på **More fields** (Flere felter).

   i. Vælg afkrydsningsfeltet for hvert felt, der kræves til logon, eller ryd afkrydsningsfelterne for hvert felt, der ikke kræves til logon.

   ii. Hvis Password Manager ikke kan detektere alle logonfelterne, vises en meddelelse, der spørger, om du vil fortsætte. Klik på **Yes** (Ja).

   iii. Der vises en dialogboks med dine logonfelter udfyldt. Klik på ikonet for hvert felt, træk det til det relevante logonfelt, og klik derefter på knappen for at tilmelde dig webstedet.

   BEMÆRK: Når du anvender den manuelle tilstand til indtastning af logondata for et sted, skal du fortsætte med at anvende denne metode til at logge på det samme websted i fremtiden.

   BEMÆRK: Den manuelle metode til indtastning af logondata er kun tilgængelig med Internet Explorer 8.

   iv. Klik på **Close** (Luk).

Hver gang du får adgang til det pågældende websted eller åbner det pågældende program, vises ikonet for Password Manager, hvilket indikerer, at du kan bruge dine registrerede legitimationsoplysninger til at logge på.

Redigering af logonindstillinger

Sådan redigerer du en logon:

1. Åbn logonskærmbilledet for et websted eller program.
2. Klik på ikonet for **Password Manager**, og klik derefter på **Edit logon** (Rediger logon) for at få vist en dialogboks, hvor du kan redigere dine logonoplysninger. Llogonfelter på skærmbilledet, og de tilsvarende felter i dialogboksen, identificeres vha. en fed orange kant.

   Du kan også få vist denne dialogboks ved at klikke på **Edit for the desired logon** (Rediger det ønskede logon) fra fanen **Password Manager Manage** (Administrer Password Manager).
3. Rediger dine logonoplysninger.
   - For at udfylde et logonfelt med et af de præformaterede valg, skal du klikke på pilene til højre for feltet.
   - For at tilføje flere felter fra skærmbilledet til din logon, skal du klikke på **More fields** (Flere felter).
   - For at få logonfelterne udfyldt, men ikke afsendt, skal du fjerne markeringen fra afkrydsningsfeltet **Submit logon data** (Send logondata).
   - For at få vist adgangskoden for denne logon, skal du klikke på **Show password** (Vis adgangskode).
4. Klik på **OK**.

Brug af menuen Logons

Password Manager giver en hurtig, nem måde at starte websteder og programmer på, som du har oprettet logons til. Dobbeltklik på en program- eller websted-logon fra menuen **Logons** eller fanen **Manage** (Administrer) i **Password Manager** for at åbne logonskærmbilledet, og derefter udfylde med dine logondata.

Når du opretter en logon, føjes den automatisk til din Logons-menu til Password Manager.

Sådan får du vist menuen Logons:

1. Tryk på hot key-kombinationen i **Password Manager**. ctrl+Windows+h er fabriksindstillingen. Klik på **Password Manager**, og klik derefter på **Settings** (Indstillinger) for at ændre hot key-kombinationen.
2. Scan dit finderaftryk (på computere med en indbygget eller tilsluttet fingeraftrykslæser).

Organisering af logons i kategorier

Brug kategorier til at holde styr på dine logons ved at oprette en eller flere kategorier. Træk og slip derefter dine logons i de ønskede kategorier.

Sådan tilføjer du en kategori:

1. Klik på **Password Manager** fra kontrolpanelet til Security Manager.
2. Klik på fanen **Manage** (Administrer), og klik derefter på **Add Category** (Tilføj kategori).
3. Indtast et navn for kategorien.
4. Klik på **OK**.

Sådan føjer du en logon til en kategori:

1. Anbring musemarkøren over den ønskede logon.
2. Tryk på den venstre museknap, og hold den nede.
3. Træk logon til listen over kategorier. Kategorier fremhæves, efterhånden som du flytter musen hen over dem.
4. Slip museknappen, når den ønskede kategori fremhæves.

Dine logons flyttes ikke til kategorien, men kopieres kun til den valgte kategori. Du kan tilføje den samme logon til mere end én kategori, og du kan få vist alle dine logons ved at klikke på **Alle**.

Administration af dine logons

Med Password Manager er det nemt at administrere dine logonoplysninger for brugernavne, adgangskoder og flere logonkonti fra ét centralt sted.

Dine logons vises på fanen Administrer. Hvis der er oprettet flere logons til det samme websted, vises hver logon derefter under webstednavnet og på logonlisten.

Sådan administrerer du logons:

Klik på **Password Manager**, og klik derefter på fanen **Administrer** fra kontrolpanelet til Security Manager.

- **Tilføje en logon** - Klik på **Add Logon** (Tilføj logon), og følg anvisningerne på skærmen.
- **Redigere en logon** - Klik på en logon, klik på **Rediger**, og ret derefter logondataene.
- **Slette en logon** - Klik på en logon, og klik derefter på **Slet**.

Sådan føjer du en ekstra logon til et websted eller program:

1. Åbn logonskærmbilledet for webstedet eller programmet.
2. Klik på ikonet for **Password Manager** for at få vist genvejsmenuen.
3. Klik på **Add additional logon** (Tilføj flere logon) og følg anvisningerne på skærmen.

Fastsætte styrken af din adgangskode

Anvendelse af stærke adgangskoder for logon til dine websteder og programmer er et vigtigt aspekt i beskyttelse af din identitet.

Password Manager foretager nemt overvågning og forbedring af din sikkerhed med omgående og automatiske analyser af styrken af de adgangskoder, der bruges til at logge på dine websteder og programmer.

Ikonindstillinger til Password Manager

Password Manager forsøger at identificere logonskærmbilleder for websteder og programmer. Når den registrerer et logonskærmbillede, hvor du ikke har oprettet en logon, beder Password Manager dig om at tilføje en logon for skærmbillet ved at vise ikonet for Password Manager med et "+"-tegn.

Klik på ikonpilen, og klik derefter på **Icon Settings** (Ikonindstillinger) for at tilpasse, hvordan **Password Manager** håndterer mulige logon-websteder.

- **Prompt to add logons for logon screens** (Promt for at tilføje logons til logonskærmbilleder) - Klik på denne indstilling for at få Password Manager til at spørge dig, om du vil tilføje en logon, når der vises et logonskærmbillede, der ikke allerede har en logonindstilling.
- **Exclude this screen** (Udeluk dette skærmbillede) - Marker afkrydsningsfeltet, så Password Manager ikke spørge dig igen om at tilføje en logon til dette logonskærmbillede.

Klik på **Password Manager**, og klik derefter på **Settings** (Indstillinger) på kontrolpanelet til Security Manager for at på adgang til yderligere Password Manager-indstillinger.

Indstillinger

Du kan angive indstillinger for tilpasning af HP ProtectTools Security Manager:

1. **Prompt to add logons for logon screens** (Promt for at tilføje logons til logonskærmbilleder) - Ikonet for Password Manager med et plustegn vises, når der registreres et websted- eller programlogonskærmbillede, der indikerer, at du kan tilføje en logon for dette skærmbillede til adgangskodeboksen. For at deaktivere denne funktion skal du i dialogboksen **Indstillinger for ikon** fjerne markeringen fra afkrydsningsfeltet ved siden af **Prompt to add logons for logon screens** (Promt for at tilføje logons til logonskærmbilleder).
2. **Open Password Manager with ctrl+Windows+h** - (Åbn Password Manager med ctrl+alt+h) - Standard hot key, der åbner menuen Quick Links (Hurtige link) til Password Manager er ctrl+alt +h. Hvis du vil ændre hot key, skal du klikke på denne funktion og indtaste en ny tastkombination. Kombinationer kan indeholde: ctrl, alt eller shift samt enhver alfabetisk eller numerisk tast.
3. Klik på **Anvend** for at gemme ændringerne.

Legitimationsoplysninger

Du bruger legitimationsoplysningerne til Security Manager til at verificere, at det virkelig er dig. Den lokale administrator af denne computer kan opsætte, hvilke legitimationsoplysninger der skal bruges for at bevise din identitet, når der logges på til din Windows-konto, websteder eller programmer.

Tilgængelige legitimationsoplysninger kan variere afhængigt af de sikkerhedsenheder, der er indbygget eller tilsluttet din computer. Hver understøttet legitimationsoplysning har en post i gruppen **My Identity, Credentials** (Min identitet, legitimationsoplysninger).

Tilgængelige legitimationsoplysninger, krav og aktuel status vises og kan indeholde følgende:

- Fingeraftryk
- Adgangskode
- Smart Card (chipkort)
- Ansigt

Klik på linket, og følg anvisningerne på skærmen for at registrere eller ændre en legitimationsoplysning.

Dit personlige id-kort

Dit id-kort identificerer entydigt dig som ejer af denne Windows-konto ved at vise dit navn og et billede efter dit valg. Det vises tydeligt i øverste venstre hjørne på siderne til Security Manager og som en Windows sidebjælke-gadget.

At klikke på dit id-kort i sidebjælken til Windows er en af de mange måder til hurtigt at få adgang til Security Manager.

Du kan ændre billedet og den måde, som dit navn vises på. Som standard vil dit fulde Windows-brugernavn og det billede, du valgte under installation af Windows, blive vist.

Sådan ændrer du det viste navn:

1. Klik på ikonet **ID Card** (Id-kort) i øverste venstre hjørne i kontrolpanelet til Security Manager.
2. Klik på det afkrydsningsfelt, der viser det navn, du indtastede for din konto i Windows. Systemet viser dit Windows-brugernavn for denne konto.
3. Indtast det nye navn, og klik derefter på knappen **Gem** for at ændre dette navn.

Sådan ændrer du det viste billede:

1. Klik på **ID Card** (Id-kort) i øverste venstre hjørne i kontrolpanelet til Security Manager.
2. Klik på knappen **Choose picture** (Vælg billede), klik på et billede, og klik derefter på knappen **Gem**.

Indstilling af dine præferencer

Du kan personliggøre indstillinger for HP ProtectTools Security Manager: Klik på **Advanced** (Avanceret), og klik derefter på **Preferences** (Præferencer) fra kontrolpanelet til Security Manager. Tilgængelige indstillinger vises på to faner: Generelt og Fingerprint (Fingeraftryk).

Generelt

Følgende indstillinger er tilgængelige på fanen Generelt:

Appearance (Udseende) - **Show icon on taskbar** (Vis ikon på proceslinjen)

- Marker afkrydsningsfeltet for at aktivere visning af ikonet på proceslinjen.
- Fjern markeringen af afkrydsningsfeltet for at deaktivere visning af ikonet på proceslinjen.

Fingerprint (Fingeraftryk)

Følgende indstillinger er tilgængelige på fanen Fingerprint (Fingeraftryk):

- **Quick Actions** (Hurtige handlinger) – Brug Quick Actions (Hurtige handlinger) til at vælge den opgave i Security Manager, der skal udføres, når du holder en angivet tast nede, mens du scanner dit fingeraftryk.

  For at knytte en Quick Action (Hurtig handling) til en af de viste taster skal du klikke på en **(tast) + fingeraftryk**smulighed og derefter vælge en af de mulige opgaver på menuen.

- **Fingerprint Scan Feedback** (Fingeraftrykksscanning, feedback) – Vises kun, når en fingeraftrykslæser er tilgængelig. Brug denne indstilling til at justere den feedback, der sker, når du scanner dit fingeraftryk.

  - **Enable sound feedback** (Aktiver lyd, feedback) – Security Manager giver lydfeedback, når et fingeraftryk er blevet scannet, ved at afspille forskellige lyde for bestemte programbegivenheder. Du kan tildele nye lyde til disse hændelser via fanen Lyde i Kontrolpanelet i Windows eller deaktivere lydfeedback ved at fjerne denne funktion.

  - **Show scan quality feedback (Vis scanningskvalitet, feedback)**

    Vælg afkrydsningsfeltet for at vise alle scanninger, uanset kvalitet.

    Ryd afkrydsningsfeltet for kun at vise scanninger i god kvalitet.

Sikkerhedskopiering og gendannelse af dine data

Det anbefales, at du regelmæssigt sikkerhedskopierer dine Security Manager-data. Hvor tit du sikkerhedskopierer, afhænger af hvor ofte dataene ændres. Hvis du f.eks. jævnligt tilføjer nye logoer, bør du muligvis sikkerhedskopiere dine data dagligt.

Sikkerhedskopiering kan også anvendes til at overføre fra en computer til en anden, også kaldet import og eksport.

BEMÆRK: Kun data sikkerhedskopieres ved denne funktion.

HP ProtectTools Security Manager skal være installeret på enhver computer, der skal modtage sikkerhedskopierede data, før dataene kan gendannes fra sikkerhedskopifilen.

Sådan sikkerhedskopierer du data:

1. I venstre panel klikker du på **Advanced** (Avanceret) og derefter på **Backup and Restore** (Sikkerhedskopier og Gendan).
2. Klik på **Back up data** (Sikkerhedskopi af data).
3. Vælg det modul, som du vil inkludere i sikkerhedskopieringen. I de fleste tilfælde ønsker du at vælge dem alle.
4. Indtast et navn for lagerfilen. Som standard gemmes filen i mappen Dokumenter. Klik på **Browse** (Gennemse) for at angive en anden placering.
5. Indtast en adgangskode for at beskytte filen.
6. Verificer din identitet.
7. Klik på **Udfør**.

Sådan gendanner du data:

1. I venstre panel klikker du på **Advanced** (Avanceret) og derefter på **Backup and Restore** (Sikkerhedskopier og Gendan).
2. Klik på **Restore data** (Gendan data).
3. Vælg den tidligere oprettede lagerfil. Du kan indtaste stien i det angivne felt eller klikke på **Browse** (Gennemse).
4. Indtast den adgangskode, der anvendes for at beskytte filen.
5. Vælg de moduler, hvis data du vil gendanne. I de fleste tilfælde vil dette være alle de oplistede moduler.
6. Klik på **Udfør**.

Find ud af mere

Ekstra programmer med nye funktioner til dette program er muligvis tilgængelige.

Klik på **[+] Discover more** (Se mere) for at gennemse flere programmer fra kontrolpanelet til Security Manager.

BEMÆRK: Hvis der ikke er noget **[+] Discover more** (Se mere) link i den nederste venstre del af kontrolpanelet, er det blevet deaktiveret af administratoren af denne computer.

Opdateringer og meddelelser

1. Marker afkrydsningsfeltet **Keep me informed about new applications and updates** (Hold mig informeret om nye programmer og opdateringer) for at anmode om information om nye programmer og opdateringer.
2. Vælg antallet af dage for at opsætte en plan over automatiske opdateringer.
3. Klik på **Kontroller nu** for at kontrollere, om der er kommet opdateringer.

Status for sikkerhedsprogram

Siden Security Manager Applications Status (Programstatus til Security Manager) viser den samlede status af dine installerede sikkerhedsprogrammer. Siden viser de programmer, der er installeret, og installationsstatus for hver. Oversigten vises automatisk, når du åbner kontrolpanelet til Security Manager og klikker på **Check the status of the security applications** (Kontroller status for sikkerhedsprogrammer), når du klikker på **Security Applications** (Sikkerhedsprogrammer), eller når du klikker på **Check Now** (Kontroller nu) på ikonet **Gadget** (Gadget) i Windows sidepanelet til højre på skærmen.

8 Drevkryptering til HP ProtectTools (kun udvalgte modeller)

△ **FORSIGTIG:** Hvis du beslutter dig for at afinstallere Drive Encryption-modulet, skal du først dekryptere alle krypterede drev. Gør du ikke det, vil du ikke kunne få adgang til dataene på krypterede drev, medmindre du har tilmeldt dig Drive Encryption-gendannelsestjenesten. Geninstallation af Drive Encryption-modulet gør det ikke muligt for dig at få adgang til de krypterede drev.

Drevkryptering til HP ProtectTools indeholder komplet databeskyttelse ved at kryptere din computers harddisk. Når Drive Encryption aktiveres, skal du logge ind på Drive Encryptions logonskærmbillede, der vises, før Windows®-operativsystemet starter.

Guiden Installation til HP ProtectTools giver Windows-administratorer mulighed for at aktivere drevkryptering), sikkerhedskopiering af krypteringsnøglen, tilføjelse og fjernelse af brugere samt deaktivering af drevkryptering. Se Hjælp i programmet HP ProtectTools Security Manager for yderligere oplysninger.

Følgende opgaver kan udføres med diskkryptering:

- Encryption Management

  Kryptering og dekryptering af individuelle drev

  BEMÆRK: Kun interne harddiske kan krypteres.

- Genoprettelse
  - Oprettelse af sikkerhedskopinøgler
  - Udførelse af en genoprettelse

Opsætningsprocedurer

Åbning af Drevkryptering

1. Klik på **Start**, klik på **Alle programmer**, klik på **HP** og klik derefter på **HP ProtectTools Administrative Console**.
2. I venstre rude skal du klikke på **Drevkryptering**.

Generelle opgaver

Aktivering af Drevkryptering

Anvend guiden Installation til HP ProtectTools til at aktivere Drevkryptering.

BEMÆRK: Denne guide anvendes også til at tilføje og fjerne brugere.

- eller -

1. Klik på **Start**, klik på **Alle programmer**, klik på **HP** og klik derefter på **HP ProtectTools Administrative Console**.
2. I venstre rude skal du klikke på **Security** (Sikkerhed) og derefter klikke på **Features** (Funktioner).
3. Markér afkrydsningsfeltet **Drevkryptering**, og klik derefter på **Næste**.
4. Under **Drives to be encrypted** (Drev, der skal krypteres) skal du markere afkrydsningsfeltet for den harddisk, du vil kryptere.
5. Sæt lagerenheden i den relevante slot.

   BEMÆRK: For at gemme den krypterede nøgle skal du anvende en USB-lagerenhed med FAT32-formatet.

6. Under **External storage device on which to save encryption key** (Ekstern lagerenhed, hvor du vil gemme krypteringsnøglen) skal du markere afkrydsningsfeltet for lagerenheden, hvor den krypterede nøgle vil blive gemt.
7. Klik på **Anvend**.

   Drevkryptering starter.

Se Hjælp i programmet HP ProtectTools Security Manager for yderligere oplysninger.

Deaktivering af Drevkryptering

Anvend guiden Installation til HP ProtectTools til at deaktivere Drevkryptering. Se Hjælp i programmet HP ProtectTools Security Manager for yderligere oplysninger.

- eller -

1. Klik på **Start**, klik på **Alle programmer**, klik på **HP** og klik derefter på **HP ProtectTools Administrative Console**.
2. I venstre rude skal du klikke på **Security** (Sikkerhed) og derefter klikke på **Features** (Funktioner).
3. Fjern markeringen fra afkrydsningsfeltet **Drevkryptering**, og klik derefter på **Anvend**.

   Diskdrevkryptering starter.

Logge på, efter at Drevkryptering er aktiveret

Når du tænder for computeren, efter at Drive Encryption er aktiveret, og din brugerkonto er registreret, skal du logge på via logonskærmen for Drive Encryption:

BEMÆRK: Hvis Windows-administratoren har aktiveret Pre-boot Security i HP ProtectTools Security Manager, logger du ind på computeren straks efter, at computeren tændes i stedet for i logonskærmen for Drive Encryption.

1. Klik på dit brugernavn, og indtast derefter din Windows-adgangskode eller Java™ Card-PIN-kode, eller før en registreret finger ned over sensoren.
2. Klik på **OK**.

BEMÆRK: Hvis du bruger en genoprettelsestast til at logge ind på logonskærmen for Drive Encryption, bliver du også bedt om at vælge dit Windows-brugernavn og angive din adgangskode på Windows-logonskærmen.

Beskyt dine data ved at kryptere din harddisk

Anvend guiden Installation til HP ProtectTools for at beskytte dine data ved at kryptere din harddisk:

1. Klik på **Sådan kommer du i gang**, og klik derefter på ikonet for **Security Manager Setup** (Installation af Security Manager). En demonstration, der beskriver funktionerne i Security Manager starter. (Du kan også starte Security Manager fra siden Drevkryptering).
2. I venstre rude klikker du på **Drive Encryption** (Drevkryptering) og klik dernæst **Encryption Management** (Håndtering af kryptering).
3. Klik på **Change Encryption** (Skift kryptering).
4. Vælg den disk eller diske, der skal krypteres.

BEMÆRK: Det anbefales på det kraftigste, at du krypterer harddisken.

Visning af krypteringsstatus

Brugere kan få vist krypteringsstatus fra HP ProtectTools Security Manager.

BEMÆRK: Ændringer af diskkrypteringsstatus skal foretages ved hjælp af HP ProtectTools Administrative Console.

1. Åbn **HP ProtectTools Security Manager**.
2. Klik på **Encryption Status** (Krypteringsstatus) under **My Data** (Mine data).

   Hvis Drevkryptering aktiveres, viser diskstatus en af de følgende statuskoder:

   - Active (Aktiv)
   - Inactive (Inaktiv)
   - Not encrypted (Ikke krypteret)
   - Encrypted (Krypteret)
   - Encrypting (Kryptering)
   - Drevkryptering

   Hvis harddisken er under kryptering eller dekryptering, vises en statuslinje med procentvis udførelse og tilbageværende tid, før krypteringen eller dekrypteringen er færdig

Avancerede opgaver

Administrering af Drive Encryption (administratoropgave)

På siden Encryption Management kan administratorer få vist og ændre status for Drevkryptering (aktiv eller inaktiv) og få vist krypteringsstatus for alle computerens harddiske.

- Hvis status er Inactive (Inaktiv), er Drevkryptering endnu ikke aktiveret i HP ProtectTools Security Manager af Windows-administratoren og beskytter ikke harddisken. Anvend guiden Installation til HP ProtectTools Security Manager til at aktivere Drevkryptering.
- Hvis status er Active (Aktiv), er Drevkryptering blevet aktiveret og konfigureret. Disken har en af følgende status:
  - Not encrypted (Ikke krypteret)
  - Encrypted (Krypteret)
  - Encrypting (Kryptering)
  - Drevkryptering

Kryptering og dekryptering af individuelle drev

For at kryptere en eller flere harddiske på computeren eller dekryptere en disk, der allerede er blevet krypteret, skal du anvende funktionen Change Encryption (Skift kryptering).

1. Åbn **HP ProtectTools Administrative Console**, klik på **Drevkryptering**, og klik derefter på **Encryption Management**.
2. Klik på **Change Encryption** (Skift kryptering).
3. I dialogboksen Change Encryption (Skift kryptering) skal du markere eller fjerne markeringen i afkrydsningsfeltet ud for hver af de harddiske, som du vil kryptere eller dekryptere, og derefter klikke på **OK**.

BEMÆRK: Når drevet krypteres eller dekrypteres, viser statuslinjen den resterende tid til færdiggørelse af processen i den aktuelle session. Hvis computeren lukkes ned eller skifter til Dvale eller Standby under krypteringsprocessen og derefter genstarter, nulstilles visningen af resterende tid til starten, men den faktiske kryptering genoptages fra det sted, hvor den sidst stoppede. Visningen af resterende tid og status ændrer sig hurtigere for at afspejle den forrige status.

Sikkerhedskopiering og gendannelse (administratoropgave)

Med siden Recovery (Gendannelse) kan administratorer sikkerhedskopiere og genoprette krypteringsnøgler.

Local Drive Encryption Key Backup (Sikkerhedskopiering af krypteringsnøgle til lokal disk) - Giver mulighed for at sikkerhedskopiere krypteringsnøgler til flytbare medier, når Drevkryptering aktiveres.

Oprettelse af sikkerhedskopinøgler

Du kan sikkerhedskopiere krypteringsnøglen for en krypteret disk til en flytbar lagerenhed:

△ **FORSIGTIG:** Sørg for at opbevare den lagerenhed, som indeholder sikkerhedskopinøglen, på et sikkert sted, fordi, hvis du glemmer din adgangskode eller mister dit Java Card, er denne enhed din eneste mulighed for adgang til din harddisk.

1. Åbn **HP ProtectTools Administrative Console**, klik på **Drevkryptering**, og klik derefter på **Genoprettelse**.
2. Klik på **Backup Keys** (Sikkerhedskopinøgler).
3. På siden Select Backup Disk (Vælg sikkerhedskopidisk) skal du markere afkrydsningsfeltet for den enhed, hvor du vil sikkerhedskopiere din krypteringsnøgle, og derefter klikke på **Næste**.
4. Læs oplysningerne på den næste side, der vises, og klik derefter på **Næste**. Krypteringsnøglen gemmes på den valgte lagerenhed.
5. Klik på **Finish** (Udfør), når bekræftelsesdialogboksen åbnes.

Udførelse af en gendannelse

Sådan udfører du en genoprettelse, hvis du glemmer din adgangskode:

1. Tænd for computeren.
2. Sæt den flytbare lagerenhed, som indeholder din sikkerhedskopinøgle, i.
3. Når logondialogboksen til Drive Encryption til HP ProtectTools åbnes, skal du klikke på **Cancel** (Annuller).
4. Klik på **Options** (Indstillinger) i nederste venstre hjørne af skærmbilledet, og klik derefter på **Genoprettelse**.
5. Vælg den fil, der indeholder din sikkerhedskopinøgle, eller klik på **Browse** (Gennemse) for at søge efter den, og klik derefter på **Næste**.
6. Klik på **OK** i bekræftelsesdialogboksen, når den åbnes.

   Din computer starter.

BEMÆRK: Det anbefales på det kraftigste, at du nulstiller din adgangskode, efter at du har udført en genoprettelse.

9 Privacy Manager til HP ProtectTools (kun udvalgte modeller)

Privacy Manager til HP ProtectTools sætter dig i stand til at anvende avancerede sikkerhedslogonmetoder (godkendelse) til at verificere kilden, integriteten og sikkerheden ved kommunikation ved anvendelse af e-mail, Microsoft® Office-dokumenter eller onlinemeddelelser.

Privacy Manager udnytter optimalt den sikkerhedsinfrastruktur, der tilvejebringes af HP ProtectTools Security Manager, som omfatter følgende sikkerhedslogonmetoder:

- Fingeraftryksgodkendelse
- Windows®-adgangskode
- HP ProtectTools Java™ Card

Du kan anvende enhver af ovenstående sikkerhedslogonmetoder i Privacy Manager.

Privacy Manager kræver følgende:

- HP ProtectTools Security Manager 5.00 eller nyere
- Operativsystemet Windows® 7, Windows Vista® eller Windows XP
- Microsoft Outlook 2007 eller Microsoft Outlook 2003
- Gyldig e-mail-konto

BEMÆRK: Et Privacy Manager Certificate (et digitalt certifikat) er påkrævet og skal installeres i Privacy Manager, før du kan få adgang til sikkerhedsfunktionerne. Der henvises til Anmodning om og installation af et Privacy Manager-certifikat på side 46 vedr. oplysninger om anmodning om et Privacy Manager Certificate.

Opsætningsprocedurer

Åbning af Privacy Manager

Sådan åbnes Privacy Manager:

1. Klik på **Start**, klik på **Alle programmer**, klik på **HP** og klik derefter på **HP ProtectTools Security Manager**.
2. Klik på **Privacy Manager**.

- eller -

Højreklik på ikonet for **HP ProtectTools** i meddelelsesområdet længst til højre på proceslinjen, klik på **Privacy Manager** (Administration af personlige oplysninger), og klik derefter på **Konfiguration**.

- eller -

På værktøjslinjen i en Microsoft Outlook-e-mail-meddelelse skal du klikke på nedpilen ud for **Send Securely** (Send sikkert) og derefter klikke på **Certificates** (Certifikater) eller **Trusted Contacts** (Kontaktpersoner, der er tillid til).

- eller -

På værktøjslinjen i et Microsoft Office-dokument skal du klikke på nedpilen ud for **Sign and Encrypt** (Signer eller krypter) og derefter klikke på **Certificates** (Certifikater) eller **Trusted Contacts** (Kontaktpersoner, der er tillid til).

Administration af Privacy Manager-certifikater

Privacy Manager-certifikater beskytter data og meddelelser vha. en kryptografisk teknologi ved navn PKI (public key infrastructure, offentlig nøgleinfrastruktur). PKI kræver, at brugerne skaffer kryptografiske nøgler og et Privacy Manager-certifikat udstedt af en certifikatmyndighed (CA). I modsætning til de fleste typer datakrypterings- og godkendelsessoftware, som kun kræver, at du godkender med jævne mellemrum, kræver Privacy Manager godkendelse, hver gang du signerer en e-mail-meddelelse eller et Microsoft Office-dokument vha. en kryptografisk nøgle. Privacy Manager gør det nemt og sikkert at gemme og sende dine vigtige data.

Du kan gøre følgende:

- Anmode om og installere et Privacy Manager-certifikat
- Få vist Privacy Manager-certifikatdetaljer
- Forny Privacy Manager-certifikater
- Når der er flere tilgængelige certifikater, skal du indstille et standard Privacy Manager-certifikat, der skal anvendes af Privacy Manager
- Slet og tilbagekald et Privacy Manager-certifikat (avanceret)

Anmodning om og installation af et Privacy Manager-certifikat

Før du kan anvende funktionerne i Privacy Manager, skal du anmode om og installere et Privacy Manager-certifikat (i Privacy Manager) vha. en gyldig e-mail-adresse. E-mail-adressen skal konfigureres som en konto i Microsoft Outlook på den samme computer, som du anmoder om Privacy Manager-certifikatet fra.

Anmodning om et Privacy Manager-certifikat

1. Åbn Privacy Manager, og klik på **Certificates** (Certifikater).
2. Klik på **Request a Privacy Manager Certificate** (Anmod om et Privacy Manager-certifikat).
3. På velkomstsiden skal du læse teksten og derefter klikke på **Next** (Næste).
4. På siden License Agreement (Licensaftale) skal du læse licensaftalen.
5. Kontrollér, at afkrydsningsfeltet ud for **Check here to accept the terms of this license agreement** (Afkryds her for at acceptere betingelserne i denne licensaftale) er markeret, og klik derefter på **Næste**.
6. På siden Your Certificate Details (Detaljer om certifikatet) skal du angive de nødvendige oplysninger og derefter klikke på **Next** (Næste).
7. På siden "Certificate Request Accepted" (Certifikatanmodning accepteret) skal du klikke på**Finish** (Udfør).
8. Klik på **OK** for at lukke certifikatet.

Du vil modtage en e-mail i Microsoft Outlook med dit Privacy Manager-certifikat vedhæftet.

Hentning af et forud tildelt Privacy Manager Corporate-certifikat

1. I Outlook skal du åbne den e-mail, som du modtog, der indikerede, at et forud tildelt Corporate-certifikat er blevet tildelt dig.
2. Klik på **Obtain** (Hent).
3. Du vil modtage en e-mail i Microsoft Outlook med dit Privacy Manager-certifikat vedhæftet.
4. Se Installation af et Privacy Manager-certifikat på side 47 for at installere certifikatet.

Installation af et Privacy Manager-certifikat

1. Når du modtager e-mail'en med dit Privacy Manager-certifikat vedhæftet, skal du åbne e-mail'en og klikke på knappen **Setup** (Installer) i nederste højre hjørne af meddelelsen i Outlook 2007, eller i øverste venstre hjørne i Outlook 2003.
2. Godkend vha. din valgte sikkerhedslogonmetode.
3. På siden Certificate Installed (Certifikat installeret) skal du klikke på **Next** (Næste).
4. På siden Certificate Backup (Sikkerhedskopi af certifikat) skal du angive en placering og et navn til sikkerhedskopifilen eller klikke på **Browse** (Gennemse) for at søge efter en placering.

△ **FORSIGTIG:** Sørg for at gemme filen på et sikkert sted - et andet sted end harddisken. Denne fil skal kun anvendes af dig og er nødvendig, hvis du får brug for at gendanne dit Privacy Manager-certifikat og de tilhørende nøgler.

5. Indtast og bekræft en adgangskode, og klik derefter på **Næste**.
6. Godkend vha. din valgte sikkerhedslogonmetode.
7. Hvis du vælger at påbegynde processen med invitation af Kontaktpersoner, der er tillid til, skal du følge anvisningerne på skærmen, der starter med trin 2 i emnet Tilføjelse af Kontaktpersoner, der er tillid til ved hjælp af Microsoft Outlook-kontaktpersoner på side 51.

- eller -

Hvis du klikker på **Annuller**, kan du se oplysninger for Tilføjelse af en Kontaktperson, der er tillid til på side 50 vedr. tilføjelse af en Kontaktpersoner, der er tillid til, på et senere tidspunkt.

Visning af Privacy Manager-certifikatdetaljer

1. Åbn Privacy Manager, og klik på **Certifikater**.
2. Klik på et Privacy Manager-certifikat.
3. Klik på **Certifikatdetaljer**.
4. Når du er færdig med at se detaljerne, skal du klikke på **OK**.

Fornyelse af et Privacy Manager-certifikat

Når dit Privacy Manager-certifikat nærmer sig tiden for udløb, får du besked om, at du skal forny det:

1. Åbn Privacy Manager, og klik på **Certifikater**.
2. Klik på **Forny certifikat**.
3. Følg anvisningerne på skærmen for at købe et nyt Privacy Manager-certifikat.

BEMÆRK: Privacy Manager-certifikatfornyelsen erstatter ikke dit gamle Privacy Manager-certifikat. Du skal købe en nyt Privacy Manager-certifikat og installere det vha. de samme procedurer, som i Anmodning om og installation af et Privacy Manager-certifikat på side 46.

Indstilling af et standard Privacy Manager-certifikat

Det er kun Privacy Manager-certifikater, der er synlige i Privacy Manager, også selvom yderligere certifikater fra andre certifikatmyndigheder installeres på computeren.

Hvis du har mere end ét Privacy Manager-certifikat på din computer, som er installeret i Privacy Manager, kan du angive ét som standardcertifikat:

1. Åbn Privacy Manager, og klik på **Certificates** (Certifikater).
2. Klik på det Privacy Manager-certifikat, du vil anvende som standard, og klik derefter på **Set default** (Indstil standard).
3. Klik på **OK**.

BEMÆRK: Du skal ikke nødvendigvis anvende dit standard Privacy Manager-certifikat. I de forskellige Privacy Manager-funktioner kan du vælge at anvende et hvilket som helst af dine Privacy Manager-certifikater.

Sletning af et Privacy Manager-certifikat

Hvis du sletter et Privacy Manager-certifikat, kan du ikke åbne nogle af de filer eller få vist nogle af de data, som du har krypteret, med det pågældende certifikat. Hvis du ved et uheld har slettet et Privacy Manager-certifikat, kan du gendanne det vha. den sikkerhedskopifil, som du oprettede, da du installerede certifikatet. Der henvises til Gendannelse af et Privacy Manager-certifikat på side 49 for yderligere oplysninger.

Sådan sletter du et Privacy Manager-certifikat:

1. Åbn Privacy Manager, og klik på **Certificates** (Certifikater).
2. Klik på det Privacy Manager-certifikat, som du vil slette, og klik derefter på **Advanced** (Avanceret).
3. Klik på **Slet**.
4. Klik på **Ja**, når bekræftelsesdialogboksen åbnes.
5. Klik på **Luk**, og klik derefter på **Anvend**.

Gendannelse af et Privacy Manager-certifikat

Under installation af dit Privacy Manager-certifikat skal du oprette en sikkerhedskopi af certifikatet. Du kan også oprette en sikkerhedskopi fra siden Overflytning. Denne sikkerhedskopi kan anvendes ved overflytning til en anden computer eller til at gendanne et certifikat til den samme computer.

1. Åbn Privacy Manager, og klik på **Overflytning**.
2. Klik på **Gendan**.
3. Klik på **Browse** (Gennemse) på siden Migration File (Overflytningsfil) for at søge efter den .dppsm-fil, som du oprettede under sikkerhedskopieringsprocessen, og klik derefter på **Next** (Næste).
4. Indtast den adgangskode, som du brugte, da du oprettede sikkerhedskopien, og klik derefter på **Næste**.
5. Klik på **Udfør**.
6. Klik på **OK**.

Der henvises til Installation af et Privacy Manager-certifikat på side 47 eller Sikkerhedskopiering af Privacy Manager-certifikater og Trusted Contacts (Kontaktpersoner, der er tillid til) på side 64 for yderligere oplysninger.

Tilbagekaldelse af dit Privacy Manager-certifikat

Hvis du mener, at dit Privacy Manager-certifikats sikkerhed er blevet kompromitteret, kan du tilbagekalde dit eget certifikat:

BEMÆRK: Et tilbagekaldt Privacy Manager-certifikat slettes ikke. Certifikatet kan stadig anvendes til at få vist filer, som er krypteret.

1. Åbn Privacy Manager, og klik på **Certificates** (Certifikater).
2. Klik på **Advanced** (Avanceret).
3. Klik på det Privacy Manager-certifikat, som du vil tilbagekalde, og klik derefter på **Revoke** (Tilbagekald).
4. Klik på **Ja**, når bekræftelsesdialogboksen åbnes.
5. Godkend vha. din valgte sikkerhedslogonmetode.
6. Følg anvisningerne på skærmen.

Administration af Trusted Contacts (Kontaktpersoner, der er tillid til)

Trusted Contacts (Kontaktpersoner, der er tillid til), er brugere, med hvem du har udvekslet Privacy Manager-certifikater, hvilket har gjort det muligt at kommunikere sikkert med hinanden.

Trusted Contacts (Kontaktpersoner, der er tillid til) giver mulighed for at udføre følgende opgaver:

- Få vist detaljer om Trusted Contacts (Kontaktpersoner, der er tillid til)
- Slette Trusted Contacts (Kontaktpersoner, der er tillid til)
- Kontrollere tilbagekaldelsesstatus for Trusted Contacts (Kontaktpersoner, der er tillid til) (avanceret)

Tilføje Trusted Contacts (Kontaktpersoner, der er tillid til)

Tilføjelse af Trusted Contacts (Kontaktpersoner, der er tillid til) er en tretrins proces:

1. Du sender en e-mail-invitation til en Kontaktperson, der er tillid til.
2. Den Kontaktperson, der er tillid, til besvarer e-mail'en.
3. Du modtager e-mail-svaret fra Kontaktperson, der er tillid til, og klikker på **Accepter**.

Du kan sende Kontaktperson, der er tillid til e-mail-invitationer til individuelle modtagere, eller du kan sende invitationen til alle kontaktpersonerne i dit Microsoft Outlook-adressekartotek.

Der henvises til følgende afsnit ang. tilføjelse af Kontaktpersoner, der er tillid til.

BEMÆRK: For at svare på din invitation til at blive en Kontaktperson, der er tillid til, skal den eller de pågældende kontaktpersoner have Privacy Manager installeret på deres computere eller have den alternative klient installeret. Oplysninger om installation af den alternative klient findes på webstedet DigitalPersona på adressen http://DigitalPersona.com/PrivacyManager.

Tilføjelse af en Kontaktperson, der er tillid til

1. Åbn Privacy Manager, klik på **Trusted Contacts Manager**, og klik derefter på **Invite Contacts** (Inviter kontaktpersoner).

   - eller -

   I Microsoft Outlook: Klik på nedpilen ud for **Send Securely** (Send sikkert) på værktøjslinjen, og klik derefter på **Invite Contacts** (Inviter kontaktpersoner).

2. Hvis dialogboksen Vælg certifikat åbnes, skal du klikke på det Privacy Manager-certifikat, som du vil anvende, og derefter klikke på **OK**.

3. Når dialogboksen Trusted Contact Invitation (Invitation af kontaktperson, der er tillid til), åbnes, skal du læse teksten og derefter klikke på **OK**.

   Der genereres automatisk en e-mail.

4. Angiv en eller flere e-mail-adresser på de modtagere, som du vil tilføje som Kontaktpersoner, der er tillid til.

5. Redigér teksten, og underskriv med dit navn (valgfrit).

6. Klik på **Send**.

BEMÆRK: Hvis du ikke har hentet et Privacy Manager-certifikat, bliver du i en meddelelse informeret om, at du skal have et Privacy Manager-certifikat for at kunne sende en anmodning om at blive Kontaktperson, der er tillid til. Klik på **OK** for at starte guiden Certifikatanmodning. Der henvises til Anmodning om og installation af et Privacy Manager-certifikat på side 46 for yderligere oplysninger.

7. Godkend vha. din valgte sikkerhedslogonmetode.

BEMÆRK: Når e-mail'en modtages af den person, der inviteres til at blive Trusted Contact (Kontaktperson, der er tillid til), skal denne åbne e-mail'en og klikke på **Accepter** i nederste højre hjørne af e-mail'en og derefter klikke på **OK**, når bekræftelsesdialogboksen åbnes.

8. Når du modtager et e-mail-svar fra en modtager, der accepterer invitationen til at blive en Kontaktperson, der er tillid til, skal du klikke på **Accepter** i nederste højre hjørne af e-mail'en.

   Der åbnes en dialogboks, hvori det bekræftes, at modtageren er blevet føjet til din liste over Kontaktpersoner, der er tillid til.

9. Klik på **OK**.

Tilføjelse af Kontaktpersoner, der er tillid til ved hjælp af Microsoft Outlook-kontaktpersoner

1. Åbn Privacy Manager, klik på **Trusted Contacts Manager**, og klik derefter på **Invite Contacts** (Inviter kontaktpersoner).

   - eller -

   I Microsoft Outlook: Klik på nedpilen ud for **Send Securely** (Send sikkert) på værktøjslinjen, og klik derefter på **Invite All My Outlook Contacts** (Inviter alle mine Outlook-kontaktpersoner).

2. Når siden Trusted Contact Invitation (Kontaktperson, der er tillid til - invitation) åbnes, skal du vælge e-mail-adresserne på de modtagere, du vil tilføje som kontaktpersoner, der er tillid til, og derefter klikke på **Next** (Next).

3. Klik på **Finish** (Udfør), når siden Sending Invitation (Sender invitation) åbnes.

   Der genereres automatisk en e-mail med de valgte Microsoft Outlook-e-mail-adresser.

4. Redigér teksten, og underskriv med dit navn (valgfrit).

5. Klik på **Send**.

BEMÆRK: Hvis du ikke har hentet et Privacy Manager-certifikat, bliver du i en meddelelse informeret om, at du skal have et Privacy Manager-certifikat for at kunne sende en anmodning om at blive Kontaktperson, der er tillid til. Klik på **OK** for at starte guiden Certifikatanmodning. Der henvises til Anmodning om og installation af et Privacy Manager-certifikat på side 46 for yderligere oplysninger.

6. Godkend vha. din valgte sikkerhedslogonmetode.

BEMÆRK: Når e-mail'en modtages af den person, der inviteres til at blive Kontaktperson, der er tillid til, skal denne åbne e-mail'en og klikke på **Accepter** i nederste højre hjørne af e-mail'en og derefter klikke på **OK**, når bekræftelsesdialogboksen åbnes.

7. Når du modtager et e-mail-svar fra en modtager, der accepterer invitationen til at blive en Kontaktperson, der er tillid til, skal du klikke på **Accepter** i nederste højre hjørne af e-mail'en.

Der åbnes en dialogboks, hvori det bekræftes, at modtageren er blevet føjet til din liste over Kontaktpersoner, der er tillid til.

8. Klik på **OK**.

Visning af detaljer om Kontaktperson, der er tillid til

1. Åbn Privacy Manager, og klik på **Kontaktpersoner, der er tillid til**.
2. Klik på en Kontaktperson, der er tillid til.
3. Klik på **Detaljer om kontaktperson**.
4. Når du er færdig med at se detaljerne, skal du klikke på **OK**.

Sletning af en Kontaktperson, der er tillid til

1. Åbn Privacy Manager, og klik på **Kontaktpersoner, der er tillid til**.
2. Klik på den Kontaktperson, der er tillid til, som du vil slette.
3. Klik på **Slet kontaktperson**.
4. Klik på **Ja**, når bekræftelsesdialogboksen åbnes.

Kontrol af tilbagekaldelsesstatus for en Kontaktperson, der er tillid til

Sådan ser du, om en Kontaktperson, der er tillid til har tilbagekaldt deres Privacy Manager-certifikat:

1. Åbn Privacy Manager, og klik på **Kontaktpersoner, der er tillid til**.
2. Klik på en Kontaktperson, der er tillid til.
3. Klik på knappen **Avanceret**.

   Dialogboksen Advanced Trusted Contact Management åbnes.
4. Klik på **Kontroller tilbagekald**.
5. Klik på **Luk**.

Generelle opgaver

Du kan anvende Privacy Manager med følgende Microsoft-produkter:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Brug af Privacy Manager i Microsoft Outlook

Når Privacy Manager er installeret, vises knappen Privacy (Beskyttelse af personlige oplysninger) på værktøjslinjen i Microsoft Outlook, og knappen Send Securely (Send sikkert) vises på værktøjslinjen i hver Microsoft Outlook-e-mail-meddelelse. Når du klikker på nedpilen ud for **Privacy** (Beskyttelse af personlige oplysninger) eller **Send Securely** (Send sikkert), kan du vælge mellem følgende funktioner:

- Sign and Send (Signer og send) (kun knappen Send Securely (Send sikkert)) – Denne indstilling tilføjer en digital signatur til e-mailen og sender den, når du har godkendt ved hjælp af den valgte sikkerhedslogonmetode.
- Seal for Trusted Contacts and Send (Forsegl til kontaktpersoner, der er tillid til, og send) (kun knappen Send Securely (Send sikkert)) – Denne indstilling tilføjer en digital signatur, krypterer e-mailen og sender den, når du har godkendt ved hjælp af den valgte sikkerhedslogonmetode.
- Invite Contacts (Inviter kontaktpersoner) - Denne indstilling giver mulighed for at sende en Trusted Contact invitation (Kontaktperson, der er tillid til - invitation). Der henvises til Tilføjelse af en Kontaktperson, der er tillid til på side 50 for yderligere oplysninger.
- Invite Outlook Contacts (Inviter Outlook-kontaktpersoner) - Denne indstilling giver dig mulighed for at sende en Trusted Contact invitation (Kontaktperson, der er tillid til - invitation) til alle kontaktpersonerne i dit Microsoft Outlook-adressekartotek. Der henvises til Tilføjelse af Kontaktpersoner, der er tillid til ved hjælp af Microsoft Outlook-kontaktpersoner på side 51 for yderligere oplysninger.
- Åbn Privacy Manager-softwaren - Indstillinger for Certificates (Certifikater), Trusted Contacts (Kontaktpersoner, der er tillid til) giver dig mulighed for at åbne Privacy Manager-softwaren for at tilføje, få vist eller ændre aktuelle indstillinger. Der henvises til Konfiguration af Privacy Manager til Microsoft Outlook på side 53 for yderligere oplysninger.

Konfiguration af Privacy Manager til Microsoft Outlook

1. Åbn Privacy Manager, klik på **Indstillinger**, og klik derefter på fanen **E-mail**.

   - eller -

   På hovedværktøjslinjen i Microsoft Outlook: Klik på nedpilen ud for **Send Securely** (Send sikkert) (**Privacy** i Outlook 2003), og klik derefter på **Indstillinger**.

   - eller -

   På værktøjslinjen i en Microsoft-e-mail-meddelelse: Klik på nedpilen ud for **Send Securely** (Send sikkert), og klik derefter på **Indstillinger**.

2. Vælg de handlinger, som du vil udføre, når du sender en sikker e-mail, og klik derefter på **OK**.

Signering og afsendelse af en e-mail-meddelelse

1. I Microsoft Outlook: Klik på **Ny** eller **Besvar**.
2. Skriv din e-mail-meddelelse.
3. Klik på nedpilen ud for **Send Securely** (Send sikkert) (**Privacy** (Beskyttelse af personlige oplysninger) i Outlook 2003), og klik derefter på **Sign and Send** (Signer og send).
4. Godkend vha. din valgte sikkerhedslogonmetode.

Forsegling og afsendelse af en e-mail-meddelelse

Forseglede e-mail-meddelelser, som er digitalt signeret og forseglet (krypteret), kan kun ses af personer, som du vælger på din liste over Trusted Contacts (Kontaktpersoner, der er tillid til).

Sådan forsegles og sendes en e-mail-meddelelse til en Trusted Contact (Kontaktperson, der er tillid til):

1. I Microsoft Outlook: Klik på **Ny** eller **Besvar**.
2. Skriv din e-mail-meddelelse.
3. Klik på nedpilen ud for **Send Securely** (Send sikkert) (**Privacy** (Beskyttelse af personlige oplysninger) i Outlook 2003), og klik derefter på **Seal for Trusted Contacts and Send** (Forsegl til kontaktpersoner, der tillid til, og send).
4. Godkend vha. din valgte sikkerhedslogonmetode.

Visning af en forseglet e-mail-meddelelse

Når du åbner en forseglet e-mail-meddelelse, vises sikkerhedsangivelsen i e-mail'ens toptekst. Sikkerhedsangivelsen indeholder følgende oplysninger:

- Hvilke legitimationsoplysninger der blev anvendt til at verificere identiteten af den person, der har signeret e-mail'en
- Det produkt, som blev anvendt til at verificere legitimationsoplysninger for den person, der har signeret e-mail'en

Brug af Privacy Manager i et Microsoft Office 2007-dokument

BEMÆRK: Privacy Manager kan kun bruges sammen med Microsoft Office 2007-dokumenter.

Når du har installeret dit Privacy Manager-certifikat, vises knappen Sign and Encrypt (Signer og krypter) i højre side af værktøjslinjen i alle Microsoft Word-, Microsoft Excel- og Microsoft PowerPoint-dokumenter. Når du klikker på nedpilen ud for **Sign and Encrypt** (Signer og krypter), kan du vælge mellem følgende funktioner:

- Sign Document (Signer dokument) - Denne indstilling føjer din digitale signatur til dokumentet.
- Add Signature Line Before Signing (Tilføj signaturlinje inden signering) (kun Microsoft Word og Microsoft Excel)) - Som standard tilføjes en signaturlinje, når et Microsoft Word- eller Microsoft Excel-dokument signeres eller krypteres. Klik på **Add Signature Line** (Tilføj signaturlinje) for at fjerne afkrydsningen.
- Encrypt Document (Krypter dokument) - Denne indstilling føjer din digitale signatur til dokumentet og krypterer det.

- Remove Encryption (Fjern kryptering) - Denne indstilling fjerner krypteringen fra dokumentet.
- Åbn Privacy Manager-softwaren - Indstillinger for Certificates (Certifikater), Trusted Contacts (Kontaktpersoner, der er tillid til) giver dig mulighed for at åbne Privacy Manager-softwaren for at tilføje, få vist eller ændre aktuelle indstillinger. Der henvises til Administration af Privacy Manager-certifikater på side 46, Administration af Trusted Contacts (Kontaktpersoner, der er tillid til) på side 50 eller Konfiguration af Privacy Manager til Microsoft Office på side 55 for yderligere oplysninger.

Konfiguration af Privacy Manager til Microsoft Office

1. Åbn Privacy Manager, klik på **Settings** (Indstillinger), og klik derefter på fanen **Documents** (Dokumenter).

   - eller -

   På værktøjslinjen i et Microsoft Office-dokument: Klik på nedpilen ud for **Sign and Encrypt** (Signer og krypter), og klik derefter på **Settings** (Indstillinger.

2. Vælg de handlinger, som du vil konfigurere, og klik derefter på **OK**.

Signering af et Microsoft Office-dokument

1. I Microsoft Word, Microsoft Excel eller Microsoft PowerPoint: Opret, og gem et dokument.
2. Klik på nedpilen ud for **Sign and Encrypt** (Signer og krypter), og klik derefter på **Sign Document** (Signer dokument).
3. Godkend vha. din valgte sikkerhedslogonmetode.
4. Når bekræftelsesdialogboksen åbnes, skal du læse teksten og derefter klikke på **OK**.

Hvis du senere beslutter dig for at redigere dokumentet, skal du benytte følgende fremgangsmåde:

1. Klik på knappen **Office** i øverste venstre hjørne af skærmen.
2. Klik på **Prepare** (Forbered), og klik derefter på **Mark as Final** (Marker som færdig).
3. Klik på **Ja**, når bekræftelsesdialogboksen åbnes, og fortsæt med at arbejde.
4. Når du er færdig med redigeringen, skal du signere dokumentet igen.

Tilføjelse af en signaturlinje ved signering af et Microsoft Word- eller Microsoft Excel-dokument

Privacy Manager gør det muligt at tilføje en signaturlinje, når du signerer et Microsoft Word- eller Microsoft Excel-dokument:

1. I Microsoft Word eller Microsoft Excel: Opret, og gem et dokument.
2. Klik på menuen **Start**.
3. Klik på nedpilen ud for **Sign and Encrypt** (Signer og krypter), og klik derefter på **Add Signature Line Before Signing** (Tilføj signaturlinje inden signering).

BEMÆRK: Der vises en afkrydsning ud for Add Signature Line Before Signing (Tilføj signaturlinje inden signering), hvis denne indstilling er valgt. Indstillingen er valgt som standard.

4. Klik på nedpilen ud for **Sign and Encrypt** (Signer og krypter), og klik derefter på **Sign Document** (Signer dokument).

5. Godkend vha. din valgte sikkerhedslogonmetode.

Tilføje foreslåede underskrivere til et Microsoft Word- eller Microsoft Excel-dokument

Du kan tilføje mere end én signaturlinje til dit dokument ved at angive foreslåede underskrivere. En foreslået underskriver er en bruger, som er udpeget af ejeren af et Microsoft Word- eller Microsoft Excel-dokument til at føje en signaturlinje til dokumentet. Foreslåede underskrivere kan være dig selv eller en anden person, som du ønsker skal signere dit dokument. Hvis du f.eks. forbereder et dokument, som skal underskrives af alle medlemmer i din afdeling, kan du inkludere signaturlinjer for de pågældende brugere nederst på den sidste side i dokumentet med anvisning om at underskrive inden en bestemt dato.

Sådan tilføjes en foreslået underskriver til et Microsoft Word- eller Microsoft Excel-dokument:

1. I Microsoft Word eller Microsoft Excel: Opret, og gem et dokument.

2. Klik på menuen **Insert** (Indsæt).

3. I gruppen **Tekst** på værktøjslinjen skal du klikke på pilen ud for **Signature Line** (Signaturlinje) og derefter klikke på **Privacy Manager Signature Provider**.

   Dialogboksen Signature Setup (Signaturindstilling) åbnes.

4. Angiv navnet på den foreslåede underskriver i feltet under **Suggested signer** (Foreslået underskriver).

5. Indtast en meddelelse til den foreslåede underskriver i feltet under **Instructions to the signer** (Vejledning til underskriver).

   BEMÆRK: Denne meddelelse vises i stedet for en titel og enten slettes eller erstattes af brugerens titel, når dokumentet underskrives.

6. Markér afkrydsningsfeltet **Show sign date in signature line** (Vis dato for signering på signaturlinjen) for at vise datoen.

7. Markér afkrydsningsfeltet **Show signer's title in signature line** (Vis underskrivers titel på signaturlinjen) for at vise titlen.

   BEMÆRK: Fordi ejeren af dokumentet tildeler foreslåede underskrivere til sit dokument, hvis afkrydsningsfelterne **Show sign date in signature line** (Vis dato for signering på signaturlinjen) og/eller **Show signer's title in signature line** (Vis underskrivers titel på signaturlinjen) ikke er markeret, vil den foreslåede underskriver ikke kunne få vist datoen og/eller titlen på signaturlinjen, selvom den foreslåede underskrivers dokumentindstillinger er konfigureret til dette.

8. Klik på **OK**.

Tilføjelse af en foreslået underskrivers signaturlinje

Når foreslåede underskrivere åbner dokumentet, vil de få vist deres navn i parentes, hvilket angiver, at deres signatur er påkrævet.

Sådan signeres dokumentet:

1. Dobbeltklik på den relevante signaturlinje.

2. Godkend vha. din valgte sikkerhedslogonmetode.

Signaturlinjen vises i henhold til de indstillinger, der er angivet af ejeren af dokumentet.

Kryptering af et Microsoft Office-dokument

Du kan kryptere et Microsoft Office-dokument for dig selv og for dine Trusted Contacts (Kontaktpersoner, der er tillid til). Når du krypterer et dokument og lukker det, skal du og den eller de Trusted Contact(s) (Kontaktperson/Kontaktperson, der er tillid til), som du vælger på listen, godkende, inden det åbnes.

Sådan krypteres et Microsoft Office-dokument:

1. I Microsoft Word, Microsoft Excel eller Microsoft PowerPoint: Opret, og gem et dokument.
2. Klik på menuen **Start**.
3. Klik på nedpilen ud for **Sign and Encrypt** (Signer og krypter), og klik derefter på **Encrypt Document** (Krypter dokument).

   Dialogboksen Select Trusted Contacts (Vælg kontaktpersoner, der er tillid til), åbnes.
4. Klik på navnet på en Trusted Contact (Kontaktperson, der er tillid til), som skal kunne åbne dokumentet og få vist dets indhold.

BEMÆRK: Hvis du vil vælge flere navne på Trusted Contact (Kontaktpersoner, der er tillid til), skal du holde tasten ctrl nede, mens du klikker på de enkelte navne.

5. Klik på **OK**.

Hvis du senere beslutter dig for at redigere dokumentet, skal du følge proceduren i Fjernelse af krypteringen fra et Microsoft Office-dokument på side 57. Når krypteringen fjernes, kan du redigere dokumentet. Følg anvisningerne i dette afsnit for at kryptere dokumentet igen.

Fjernelse af krypteringen fra et Microsoft Office-dokument

Når du fjerner krypteringen fra et Microsoft Office-dokument, skal du og dine Trusted Contacts (Kontaktpersoner, der er tillid til), ikke længere godkende for at åbne og få vist indholdet af dokumentet.

Sådan fjerner du krypteringen fra et Microsoft Office-dokument:

1. Åbn et krypteret Microsoft Word-, Microsoft Excel- eller Microsoft PowerPoint-dokument.
2. Godkend vha. din valgte sikkerhedslogonmetode.
3. Klik på menuen **Start**.
4. Klik på nedpilen ud for **Sign and Encrypt** (Signer og krypter), og klik derefter på **Remove Encryption** (Fjern kryptering).

Afsendelse af et krypteret Microsoft Office-dokument

Du kan vedhæfte et krypteret Microsoft Office-dokument til en e-mail-meddelelse uden at signere eller kryptere selve e-mail'en. For at gøre dette skal du oprette og sende en e-mail med et signeret eller krypteret dokument på samme måde, som du ville gøre med en almindelig e-mail med en vedhæftet fil.

Det anbefales dog med henblik på optimal sikkerhed, at du krypterer e-mail'en, når du vedhæfter et signeret eller krypteret Microsoft Office-dokument.

Hvis du vil sende en forseglet e-mail med et vedhæftet, signeret og/eller krypteret Microsoft Office-dokument, skal du benytte følgende fremgangsmåde:

1. I Microsoft Outlook: Klik på **Ny** eller **Besvar**.
2. Skriv din e-mail-meddelelse.
3. Vedhæft Microsoft Office-dokumentet.
4. Der henvises til Forsegling og afsendelse af en e-mail-meddelelse på side 54 for yderligere anvisninger.

Visning af et signeret Microsoft Office-dokument

BEMÆRK: Du behøver ikke at have et Privacy Manager-certifikat for at få vist et signeret Microsoft Office-dokument.

Når et signeret Microsoft Office-dokument åbnes, vises et digital signatur-ikon på statuslinjen nederst i dokumentvinduet.

1. Klik på ikonet for **Digital signatur** for at ændre visning af signaturdialogen, der viser navnet på alle de brugere, der signerede dokumentet og datoen for, hvornår hver bruger signerede det.
2. Højreklik på et navn i signaturdialogen og vælg Signature Details (Signaturdetaljer) for at få vist yderligere detaljer om hver signatur.

Visning af et krypteret Microsoft Office-dokument

For at få vist et krypteret Microsoft Office-dokument fra en anden computer, skal Privacy Manager være installeret på den pågældende computer. Desuden skal du gendanne det Privacy Manager-certifikat, som blev anvendt til at kryptere filen.

En Trusted Contact (Kontaktperson, der er tillid til), som ønsker at se et krypteret Microsoft Office-dokument, skal have et Privacy Manager-certifikat, og Privacy Manager skal være installeret på den pågældendes computer. Desuden skal den pågældende Trusted Contact (Kontaktperson, der er tillid til), være valgt af ejeren af det krypterede Microsoft Office-dokument.

Brug af Privacy Manager i Windows Live Messenger

Privacy Manager tilføjer følgende sikre kommunikationsfunktioner til Windows Live Messenger:

- **Secure chat** (Sikker chat) - Meddelelser transmitteres ved hjælp af SSL/TLS (Secure Sockets Layer/Transport Layer Security) via XML-protokol, der er den samme teknologi, som håndterer sikkerheden ved e-handel-transaktioner.
- **Recipient identification** (Modtageridentifikation) - Du kan verificere tilstedeværelsen og identiteten af en person, før afsendelse af en meddelelse.
- **Signed messages** (Signerede meddelelser) - Du kan signere dine meddelelser elektronisk. Hvis der derefter manipuleres med meddelelsen, bliver den markeret som ugyldig, når modtageren får den.
- **Hide/show feature** (Skjul/vis funktion) - Du kan skjule et eller alle meddelelser i chatvinduet til Privacy Manager. Du kan også sende en meddelelse, hvor indholdet er skjult. Der kræves godkendelse, før meddelelsen vises.

- **Secure chat history** (Sikker chathistorik) - Logføringer af dine chatsessioner krypteres, før de gemmes og kræver godkendelse for at blive vist.
- **Automatic locking/unlocking** (Automatisk låsning/oplåsning) - Du kan låse chatvinduet til Privacy Manager og låse det op eller indstille det til at låse automatisk efter en bestemt periode med inaktivitet.

Start af en chatsession til Privacy Manager

BEMÆRK: For at kunne bruge Privacy Manager Chat skal begge parter have Privacy Manager og et Privacy Manager-certifikat installeret. Oplysninger om installation af et Privacy Manager-certifikat, se Anmodning om og installation af et Privacy Manager-certifikat på side 46.

1. Benyt en af følgende fremgangsmåder for at starte Privacy Manager Chat i Windows Live Messenger:

   a. Højreklik på en onlinekontakt i Live Messenger, og vælg derefter **Start en aktivitet**.

   b. Klik på **Start chat**.

   - eller -

   a. Dobbeltklik på en onlinekontaktperson i Live Messenger, og vælg derefter menuen **Se en liste over aktiviteter**.

   b. Klik på **Handling**, og klik derefter på **Start chat**.

   - eller -

   a. Højreklik på ikonet **ProtectTools** i meddelelsesområdet, klik på **Privacy Manager for HP ProtectTools** (Privacy Manager til HP ProtectTools), og vælg derefter **Start Chat** (Start chat).

   b. I Live Messenger: Klik på **Handlinger: Start en aktivitet**, og klik derefter på **Privacy Manager Chat**.

   BEMÆRK: Hver bruger skal være online i Live Messenger, og brugerne skal vises i de andres Live Messenger onlinevindue. Klik for at vælge en onlinebruger.

   Privacy Manager sender en invitation til kontaktpersonen om at starte Privacy Manager Chat. Når den inviterede kontaktperson accepterer, åbnes vinduet Privacy Manager Chat. Hvis den inviterede kontaktperson ikke har Privacy Manager, bliver denne bedt om at downloade det.

2. Klik på **Start** for at påbegynde en sikker chat.

Konfiguration af Privacy Manager til Windows Live Messenger

1. I Privacy Manager Chat: Klik på knappen **Settings** (Indstillinger).

   - eller -

   I Privacy Manager: Klik på **Settings** (Indstillinger), og klik derefter på fanen **Chat**.

   - eller -

   I Privacy Manager Live Messenger History Viewer: Klik på knappen **Settings** (Indstillinger).

2. Hvis du vil angive, hvor længe Privacy Manager Chat (Chat i Privacy Manager) skal vente, før din session låses, skal du vælge et tal på listen **Lock session after _ minutes of inactivity** (Lås session efter _ minutters inaktivitet).

3. Hvis du vil angive en historikmappe til dine chatsessioner, skal du klikke på **Gennemse** for at søge efter en mappe og derefter klikke på **OK**.

4. Hvis du automatisk vil kryptere og gemme dine sessioner, når du lukker dem, skal du markere afkrydsningsfeltet **Automatically save secure chat history** (Gem automatisk sikker chathistorik).

5. Klik på **OK**.

Chatte i Privacy Manager chat-vinduet

Når du har startet Privacy Manager Chat, åbnes vinduet Privacy Manager Chat i Windows Live Messenger. Brug af Privacy Manager Chat ligner brug af grundlæggende Windows Live Messenger, bortset fra, at følgende yderligere funktioner er tilgængelige i vinduet Privacy Manager Chat:

- **Gem** - Klik på denne knap for at gemme din chatsession i den mappe, du har angivet i dine konfigurationsindstillinger. Du kan også konfigurere Privacy Manager Chat (Chat i Privacy Manager) til automatisk at gemme hver session, når den lukkes.
- **Skjul alle** og **Vis alle** - Klik på den relevante knap for at udvide eller skjule de meddelelser, der vises i vinduet Secure Communikations (Sikker kommunikation). Du kan også skjule eller vise individuelle meddelelser ved at klikke på meddelelseshovedet.
- **Are you there? (Er du der?)** - Klik på denne knap for at anmode om godkendelse fra din kontaktperson.
- **Lock** (Lås) – Klik på denne knap for at lukke vinduet Privacy Manager Chat (Chat i Privacy Manager) og vende tilbage til vinduet Chat Entry (Chatpunkt). For at få vist vinduet Secure Communications (Sikker kommunikation) igen skal du klikke på **Resume the session (Genoptag sessionen)** og derefter godkende vha. din valgte sikkerhedslogonmetode.
- **Send** - Klik på denne knap for at sende en krypteret meddelelse til din kontaktperson.
- **Send signed** (Send signeret) - Markér dette afkrydsningsfelt for elektronisk at signere og kryptere dine meddelelser. Hvis der derefter manipuleres med meddelelsen, bliver den markeret som ugyldig, når modtageren får den. Du skal godkende, hver gang du sender en signeret meddelelse.
- **Send hidden** (Send skjult) - Markér dette afkrydsningsfelt for at kryptere og sende en meddelelse, hvor kun meddelelseshovedet vises. Din kontaktperson skal godkende for at læse indholdet af meddelelsen.

Visning af chathistorik

Privacy Manager Chat: Live Messenger History Viewer viser krypterede chatsessionsfiler til Privacy Manager. Du kan gemme sessioner ved at klikke på **Gem** i vinduet Privacy Manager Chat (Chat i Privacy Manager) eller ved at konfigurere automatisk lagring under fanen Chat i Privacy Manager. I fremviseren viser hver session (krypteret) Contact Screen Name (Kontaktskærmsnavnet) samt dato og klokkeslæt for påbegyndelse og afslutning af sessionen. Sessioner vises som standard for alle e-mail-konti, som du har konfigureret. Du kan bruge menuen **Display history for** (Vis historik for) for at vælge, at kun specifikke konti skal vises.

Fremviseren giver mulighed for at udføre følgende opgaver:

- Vis alle sessioner på side 61
- Vis sessioner for en bestemt konto på side 61
- Få vist et sessions-id på side 62

- Vis en session på side 62
- Søg i sessioner efter bestemt tekst på side 62
- Slet en session på side 62
- Tilføj eller fjern kolonner på side 62
- Filtrer viste sessioner på side 63

Sådan starter du Live Messenger History Viewer:

▲ Højreklik på ikonet for **HP ProtectTools** i meddelelsesområdet længst til højre på proceslinjen, klik på **Privacy Manager: for HP ProtectTools**, og klik derefter på **Live Messenger History Viewer**.

- eller -

▲ I en chatsession: Klik på **History Viewer** (Historikfremviser) eller **History** (HIstorik).

Vis alle sessioner

Med funktionen til visning af alle sessioner vises det/de dekrypterede kontaktskærmsnavn(e) for den eller de aktuelt valgte sessioner og alle sessioner for samme konto.

Sådan får du vist alle dine gemte chathistoriksessioner:

1. I Live Messenger History Viewer: Højreklik på en vilkårlig session, og vælg derefter **Reveal All Sessions** (Vis alle sessioner).
2. Godkend vha. din valgte sikkerhedslogonmetode.

   Kontaktskærmsnavnene dekrypteres.
3. Dobbeltklik på en hvilken som helst session for at få vist dens indhold.

Vis sessioner for en bestemt konto

Ved visning af en session vises det dekrypterede kontaktskærmsnavn for den aktuelt valgte session.

Sådan får du vist en specifik chathistoriksession:

1. I Live Messenger History Viewer: Højreklik på en vilkårlig session, og vælg derefter **Reveal Session** (Vis session).
2. Godkend vha. din valgte sikkerhedslogonmetode.

   Kontaktskærmsnavnet dekrypteres.
3. Dobbeltklik på den viste session for at få vist dens indhold.

BEMÆRK: For yderligere sessioner, der er krypteret med samme certifikat, vises et oplåst ikon, hvilket angiver, at du kan få dem vist ved at dobbeltklikke på enhver af de pågældende sessioner uden yderligere godkendelse. For sessioner, der er krypteret med et andet certifikat, vises et låst ikon, hvilket angiver, at der kræves yderligere godkendelse til de pågældende sessioner for at kunne få vist kontaktskærmsnavnene eller indhold.

Få vist et sessions-id

Sådan får du vist et sessions-id:

- I Live Messenger History Viewer: Højreklik på vilkårlig vist session, og vælg **View session ID** (Se sessions-id).

Vis en session

Med funktionen til visning af en session åbnes filen for visning. Hvis sessionen ikke er blevet vist (visning af det dekrypterede kontaktskærmsnavn) tidligere, vises det samtidigt.

Sådan får du vist en historiksession til Live Messenger:

1. I Live Messenger History Viewer: Højreklik på en vilkårlig session, og vælg derefter **View** (Vis).
2. Hvis du bliver bedt om det, skal du godkende vha. din valgte sikkerhedslogonmetode.

   Sessionsindholdet dekrypteres.

Søg i sessioner efter bestemt tekst

Du kan kun søge efter tekst i viste (dekrypterede) sessioner, som vises i fremviservinduet. Det er de sessioner, hvor kontaktskærmsnavnet vises som almindelig tekst.

Sådan søger du efter tekst i chathistoriksessioner:

1. I Live Messenger History Viewer: Klik på knappen **Search** (Søg).
2. Indtast søgeteksten, konfigurér eventuelt ønskede søgeparametre, og klik derefter på **OK**.

   Sessioner, som indeholder teksten, er fremhævet i fremviservinduet.

Slet en session

1. Vælg en chathistoriksession.
2. Klik på **Slet**.

Tilføj eller fjern kolonner

Som standard vises de tre oftest anvendte kolonner i Live Messenger History Viewer. Du kan føje yderligere kolonner til visningen, eller du kan fjerne kolonner fra visningen.

Sådan føjer du kolonner til visningen:

1. Højreklik på en hvilken som helst kolonneoverskrift, og vælg derefter **Tilføj/fjern kolonner**.
2. Vælg en kolonneoverskrift i det venstre panel, og klik derefter på **Tilføj** for at flytte den til det højre panel.

Sådan fjerner du kolonner fra visningen:

1. Højreklik på en hvilken som helst kolonneoverskrift, og vælg derefter **Tilføj/fjern kolonner**.
2. Vælg en kolonneoverskrift i det højre panel, og klik derefter på **Fjern** for at flytte den til det venstre panel.

Filtrer viste sessioner

Der vises en liste over sessioner for alle dine konti i Live Messenger History Viewer. Du kan også filtrere viste sessioner for følgende:

- Specifikke konti. Der henvises til Visning af sessioner for en bestemt konto på side 63 for detaljerede oplysninger.
- Interval af datoer. Der henvises til Visning af sessioner for et interval af datoer på side 63 for detaljerede oplysninger.
- Forskellige mapper. Der henvises til Visning af sessioner, der er gemt i en anden mappe end standardmappen på side 63 for detaljerede oplysninger.

Visning af sessioner for en bestemt konto

▲ I Live Messenger History Viewer: Vælg en konto i menuen **Display history for** (Vis historik for).

Visning af sessioner for et interval af datoer

1. I Live Messenger History Viewer: Klik på ikonet for **Advanced Filter** (Avanceret filter).

   Dialogboksen Advanced Filter (Avanceret filter) åbnes.

2. Markér afkrydsningsfeltet **Display only sessions within specified date range** (Vis kun sessioner inden for specifikt datointerval).
3. I tekstboksene **From date** (Fra-dato) og **To date** (Til-dato) skal du angive dato, måned og/eller år eller klikke på pilen ud for kalenderen for at vælge datoerne.
4. Klik på **OK**.

Visning af sessioner, der er gemt i en anden mappe end standardmappen

1. I Live Messenger History Viewer: Klik på ikonet for **Advanced Filter** (Avanceret filter).
2. Markér afkrydsningsfeltet **Use an alternate history files folder** (Brug en alternativ mappe til historikfiler).
3. Angiv mappens placering, eller klik på **Browse** (Gennemse) for at søge efter en mappe.
4. Klik på **OK**.

Avancerede opgaver

Overførsel af Privacy Manager-certifikater og kontaktpersoner, der er tillid til, til en anden computer

Du kan på sikker vis overføre dine Privacy Manager-certifikater og Trusted Contacts (Kontaktpersoner, der er tillid til) til en anden computer eller sikkerhedskopiere dine data til sikker opbevaring For at gøre dette skal du sikkerhedskopiere dataene som en adgangskodebeskyttet fil til en netværksplacering eller en hvilken som helst flytbar lagerenhed og derefter gendanne filen i den nye computer.

Sikkerhedskopiering af Privacy Manager-certifikater og Trusted Contacts (Kontaktpersoner, der er tillid til)

Benyt følgende fremgangsmåde for at sikkerhedskopiere dine Privacy Manager-certifikater og Trusted Contacts (Kontaktpersoner, der er tillid til), i en adgangskodebeskyttet fil:

1. Åbn Privacy Manager, og klik på **Migration** (Overflytning).
2. Klik på **Backup** (Sikkerhedskopier).
3. På siden Select Data (Vælg data) skal du vælge de datakategorier, der skal medtages i overførselsfilen og derefter klikke på **Next** (Næste).
4. På siden Migration File (Overflytningsfil) skal du angive et filnavn eller klikke på **Browse** (Gennemse) for at søge efter en placering og derefter klikke på **Next** (Næste).
5. Indtast og bekræft en adgangskode, og klik derefter på **Næste**.

BEMÆRK: Gem denne adgangskode på et sikkert sted, for du får brug for den, når du skal gendanne overførselsfilen.

6. Godkend vha. din valgte sikkerhedslogonmetode.
7. Klik på **Finish** (Udfør) på siden Migration File Saved (Overflytningsfil gemt).

Gendannelse af Privacy Manager-certifikater og Kontaktpersoner, der er tillid til

Følg nedenstående trin for at gendanne Privacy Manager-certifikater og Kontaktpersoner, der er tillid til på en anden computer som del af overførselsprocessen eller til samme computer.

1. Åbn Privacy Manager, og klik på **Overflytning**.
2. Klik på **Gendan**.
3. På siden Migration File (Overflytningsfil) skal du klikke på **Browse** (Gennemse) for at søge efter filen og derefter klikke på **Next** (Næste).
4. Indtast den adgangskode, som du brugte, da du oprettede sikkerhedskopien, og klik derefter på **Næste**.
5. Klik på **Finish** (Udfør) på siden Migration File Import (Import af overflytningsfil).

Central administration af Privacy Manager

Din installation af Privacy Manager kan være en del af en centraliseret installation, der er blevet tilpasset af din administrator. En eller flere af følgende funktioner kan enten være aktiveret eller deaktiveret:

- **Certificate use policy** (Politik ved brug af certifikat) - Du er muligvis begrænset i brugen af Privacy Manager-certifikater, der er udstedt af Comodo, eller du kan have tilladelse til at bruge digitale certifikater, der er udstedt af andre certifikatmyndigheder.
- **Encryption policy** (Krypteringspolitik) - Krypteringskapaciteter kan være individuelt aktiveret eller deaktiveret i Microsoft Office eller Outlook og i Windows Live Messenger.

10 File Sanitizer til HP ProtectTools

File Sanitizer er et værktøj, der gør det muligt for dig på sikker vis at "makulere" aktiver (personlige oplysninger eller filer, historiske eller webrelaterede data eller andre datakomponenter) på din computer og til jævnligt at rense din harddisk.

BEMÆRK: Denne version af File Sanitizer understøtter kun systemharddisken.

Makulering

Makulering er anderledes end en standard Windows®-sletning (også kaldet simpel sletning i File Sanitizer) på den måde, at når du makulerer et aktiv med File Sanitizer, aktiveres en algoritme, som tilslører dataene, hvilket gør det stort set umuligt at genfinde det oprindelige aktiv. En simpel sletning i Windows kan efterlade filen (eller aktivet) intakt på harddisken eller i en tilstand, hvor "retsmedicinske" metoder kunne anvendes til at gendanne filen (eller aktivet).

Når du vælger en makuleringsprofil (High Security, Medium Security eller Low Security), vælges der automatisk en foruddefineret liste over aktiver og en sletningsmetode til makuleringen. Du kan også tilpasse en makuleringsprofil, som gør det muligt at angive antallet af makuleringscyklusser, hvilke aktiver, der skal medtages til makulering, hvilke aktiver, der skal bekræftes forud for makulering, og hvilke aktiver, der skal udelades fra makulering. Yderligere oplysninger finder du i Valg eller oprettelse af en makuleringsprofil på side 70.

Du kan opsætte en automatisk makuleringsplan, og du kan også makulere aktiver manuelt når som helst, du ønsker det. Yderligere oplysninger finder du i Angivelse af en makuleringsplan på side 69, Manuel makulering af ét aktiv på side 74 eller Manuel makulering af alle valgte elementer på side 74.

BEMÆRK: En .dll-fil makuleres og fjernes kun fra systemet, hvis den er blevet flyttet til papirkurven.

Rensning af ledig plads

Sletning af et aktiv i Windows fjerner ikke aktivets indhold helt fra harddisken. Windows sletter kun henvisningen til aktivet. Aktivets indhold forbliver på harddisken, indtil et andet aktiv overskriver det samme område på harddisken med nye oplysninger.

Rensning af ledig plads gør det muligt på sikker vis at skrive vilkårlige data over slettede aktiver, hvilket forhindrer brugere i at se det oprindelige indhold af det slettede aktiv.

BEMÆRK: Rensning af ledig plads er for de aktiver, som du sletter vha. papirkurven i Windows, eller når du sletter et aktiv manuelt. Rensning af ledig plads giver ikke yderligere sikkerhed for makulerede aktiver.

Du kan angive en plan for automatisk rensning af ledig plads, eller du kan manuelt aktivere rensning af ledig plads vha. ikonet for **HP ProtectTools** i meddelelsesområdet længst til højre på proceslinjen. Yderligere oplysninger finder du i Angivelse af en plan for rensning af ledig plads på side 70 eller Manuel aktivering af rensning af ledig plads på side 75.

Opsætningsprocedurer

Åbning af File Sanitizer

Sådan åbnes File Sanitizer:

1. Klik på **Start**, klik på **Alle programmer**, klik på **HP** og klik derefter på **HP ProtectTools Security Manager**.
2. Klik på **File Sanitizer**.

- eller -

▲ Dobbeltklik på ikonet for **File Sanitizer**, der findes på din stationære computer.

- eller -

▲ Højreklik på ikonet for **HP ProtectTools** i meddelelsesområdet længst til højre på proceslinjen, klik på **File Sanitizer**, og klik derefter på **Open File Sanitizer** (Åbn File Sanitizer).

Angivelse af en makuleringsplan

BEMÆRK: Der henvises til Valg eller oprettelse af en makuleringsprofil på side 70 for oplysninger om valg af foruddefineret makuleringsprofil eller oprettelse af en markeret profil.

BEMÆRK: Oplysninger om manuelle makuleringsaktiver finder du under Manuel makulering af ét aktiv på side 74.

1. Åbn File Sanitizer, og klik på **Shred** (Makuler).
2. Vælg en makuleringsindstilling:
   - **Windows shutdown** (Nedlukning af Windows) - Vælg denne indstilling, hvis alle valgte aktiver skal makuleres, når Windows lukker ned.

     BEMÆRK: Når denne indstilling er valgt, åbnes der en dialogboks ved nedlukning, hvori du bliver spurgt, om du vil fortsætte med makulering af de valgte aktiver, eller om du vil omgå proceduren. Klik på **Ja**, hvis du vil omgå makuleringsproceduren, eller klik på **Nej**, hvis du vil fortsætte med makuleringen.

   - **Web browser open** - (Webbrowser, åben) - Vælg denne indstilling, hvis alle valgte, webrelaterede aktiver, som f.eks. browser-URL-historik, skal makuleres, når du åbner en webbrowser.
   - **Web browser quit** - (Webbrowser, afslut) - Vælg denne indstilling, hvis alle valgte, webrelaterede aktiver, som f.eks. browser-URL-historik, skal makuleres, når du lukker en webbrowser
   - **Tasterækkefølge** - Vælg denne indstilling for at starte makulering ved hjælp af en tastesekvens.
   - **Scheduler** (Planlægger) - Markér afkrydsningsfeltet **Activate Scheduler** (Aktiver Planlægger), indtast din Windows-adgangskode, og angiv derefter dato og klokkeslæt for makulering af de valgte aktiver.

BEMÆRK: En .dll-fil makuleres og fjernes kun fra systemet, hvis den er blevet flyttet til papirkurven.

3. Klik på **Anvend**, og klik derefter på **OK**.

Angivelse af en plan for rensning af ledig plads

BEMÆRK: Rensning af ledig plads er for de aktiver, som du sletter vha. papirkurven i Windows, eller for manuelt slettede aktiver. Rensning af ledig plads giver ikke yderligere sikkerhed for makulerede aktiver.

Sådan angiver du en plan for rensning af ledig plads:

1. Åbn File Sanitizer, og klik på **Free Space Bleaching** (Fri plads til rensning).
2. Markér afkrydsningsfeltet **Activate Scheduler** (Aktiver Planlægger), indtast din Windows-adgangskode, og angiv derefter dato og klokkeslæt for rensning af din harddisk.
3. Klik på **Anvend**, og klik derefter på **OK**.

BEMÆRK: Rensningen af ledig plads kan tage lang tid. Selvom rensning af ledig plads foregår i baggrunden, kan din computer køre langsommere på grund af den forøgede processoranvendelse.

Valg eller oprettelse af en makuleringsprofil

Du kan angive en metode til sletning og vælge de aktiver, der skal makuleres, ved at vælge en foruddefineret profil eller ved at oprette din egen profil.

Valg af en foruddefineret makuleringsprofil

Når du vælger en foruddefineret makuleringsprofil (High Security, Medium Security eller Low Security), vælges der automatisk en foruddefineret sletningsmetode og en liste over aktiver. Du kan klikke på knappen **View Details** (Vis detaljer) for at få vist den foruddefinerede liste over aktiver, der er valgt til makulering.

Sådan vælges en foruddefineret makuleringsprofil:

1. Åbn File Sanitizer, og klik på **Settings** (Indstillinger).
2. Klik på en foruddefineret makuleringsprofil.
3. Klik på **View Details** (Vis detaljer) for at få vist listen over aktiver, der er valgt til makulering.
4. Under **Shred the following** (Makulér følgende) skal du markere afkrydsningsfeltet ud for hvert aktiv, som du vil bekræfte forud for makulering.
5. Klik på **Anvend**, og klik derefter på **OK**.

Tilpasning af en makuleringsprofil

Når du opretter en makuleringsprofil, angiver du antallet af makuleringscyklusser, hvilke aktiver, der skal medtages til makulering, hvilke aktiver, der skal bekræftes forud for makulering, og hvilke aktiver, der skal udelades fra makulering:

1. Åbn File Sanitizer, og klik på **Settings** (Indstillinger), klik på **Advanced Security Settings** (Avancerede sikkerhedsindstillinger), og klik derefter på **View Details** (Vis detaljer).

2. Angiv antallet af makuleringscyklusser.

BEMÆRK: Det valgte antal makuleringscyklusser bliver udført for hvert aktiv. Hvis du f.eks. vælger tre makuleringscyklusser, udføres en algoritme, som tilslører dataene, tre forskellige gange. Hvis du vælger makuleringscyklusser med højere sikkerhed, kan makuleringen tage en del tid. Jo højere antal makuleringscyklusser, du angiver, des mindre sandsynligt er det, at dataene kan gendannes.

3. Vælg de aktiver, som du vil makulere:

   a. Klik på et aktiv under **Available shred options** (Tilgængelige makuleringsindstillinger), og klik derefter på **Add** (Tilføj).

   b. Klik på **Add Custom Option** (Tilføj tilpasset indstilling), og gennemse eller indtast derefter stien til filnavnet eller -mappen for at tilføje et tilpasset aktiv. Klik på **Open** (Åbn), og klik derefter på **OK**. Klik på det brugerdefinerede aktiv under **Available Shred Options** (Tilgængelige makuleringsindstillinger), og klik derefter på **Tilføj**.

BEMÆRK: Hvis du vil fjerne et aktiv fra de tilgængelige makuleringsindstillinger, skal du klikke på aktivet og derefter klikke på **Slet**.

4. Under **Shred the following** (Makulér følgende) skal du markere afkrydsningsfeltet ud for hvert aktiv, som du vil bekræfte forud for makulering

BEMÆRK: Hvis du vil fjerne et aktiv fra makuleringslisten, skal du klikke på aktivet og derefter klikke på **Fjern**

5. Hvis du vil beskytte filer eller mapper mod automatisk makulering, skal du under **Do not shred the following** (Følgende må ikke makuleres) klikke på **Tilføj** og derefter navigere til eller indtaste stien til filnavnet eller mappen. Klik på **Åbn**, og klik derefter på **OK**.

BEMÆRK: Hvis du vil fjerne et aktiv fra listen over udeladelser, skal du klikke på aktivet og derefter klikke på **Slet**.

6. Når du er færdig med at konfigurere makuleringsprofilen, skal du klikke på **Anvend** og derefter klikke på **OK**.

Tilpasning af en profil for simpel sletning

Med profilen for simpel sletning udføres en standardsletning af aktiver uden at makulere. Når du tilpasser en profil for simpel sletning, kan du angive, hvilke aktiver der skal medtages ved en simpel sletning, hvilke aktiver der skal bekræftes, før der udføres en simpel sletning, og hvilke aktiver der skal udelades fra en simpel sletning.

BEMÆRK: Hvis du bruger simpel sletning, kan rensning af ledig plads udføres en gang imellem på de aktiver, der er blevet slettet manuelt eller vha. Papirkurv i Windows.

Sådan tilpasser du en profil for simpel sletning:

1. Åbn File Sanitizer, klik på **Settings** (Indstillinger), klik på **Simple Delete Setting** (Indstilling for simpel sletning), og klik derefter på **View Details** (Vis detaljer).

2. Vælg de aktiver, som du vil slette:

   a. Klik på et aktiv under **Available delete options** (Tilgængelige sletningsmuligheder), og klik derefter på ´**Tilføj**.

   b. Hvis du vil tilføje et brugerdefineret aktiv, skal du klikke på **Add Custom Option** (Tilføj tilpasset indstilling), angive et filnavn eller mappenavn og derefter klikke på **OK**. Klik på det brugerdefinerede aktiv, og klik derefter på **Tilføj**.

BEMÆRK: Hvis du vil slette et aktiv fra de tilgængelige sletningsmuligheder, skal du klikke på aktivet og derefter klikke på **Slet**.

3. Under **Slet følgende** skal du markere afkrydsningsfeltet ud for hvert aktiv, som du vil bekræfte forud for sletning.

BEMÆRK: Hvis du vil fjerne et aktiv fra sletningslisten, skal du klikke på aktivet og derefter klikke på **Fjern**.

4. Klik på **Tilføj** under **Slet ikke følgende** for at vælge de bestemte aktiver, som du vil udelade fra sletningen.

BEMÆRK: Hvis du vil fjerne et aktiv fra listen over udeladelser, skal du klikke på aktivet og derefter klikke på **Slet**.

5. Når du er færdig med at konfigurere profilen for simpel sletning, skal du klikke på **Anvend** og derefter klikke på **OK**.

Generelle opgaver

Du kan anvende File Sanitizer til at udføre følgende opgaver:

- Use a key sequence to initiate shredding (Brug en tasterækkefølge for at starte makulering) - Denne funktion giver mulighed for at oprette en tasterækkefølge (f.eks. ctrl+alt+s) for at starte makulering. Der henvises til Brug af en tastesekvens for at starte makulering på side 73 for detaljerede oplysninger.
- Use the File Sanitizer icon to initiate shredding (Brug ikonet for File Sanitizer til at starte makulering - Denne funktion er lig med træk-og-sæt-ind-funktionen i Windows. Der henvises til Brug af ikonet for File Sanitizer på side 74 for detaljerede oplysninger.
- Manually shred a specific asset or all selected assets (Makulér manuelt et specifikt aktiv eller alle valgte aktiver) - Disse funktioner giver mulighed for manuelt at makulere elementer uden at vente på, at den almindelige makuleringsplan tilsløres. Der henvises til Manuel makulering af ét aktiv på side 74 eller Manuel makulering af alle valgte elementer på side 74 for detaljerede oplysninger.
- Manually activate free space bleaching (Manuel aktivering af rensning af ledig plads) - Denne funktion giver mulighed for manuelt at aktivere rensning af ledig plads. Der henvises til Manuel aktivering af rensning af ledig plads på side 75 for detaljerede oplysninger.
- Abort a shred or free space bleaching operation (Afbryd en makulerings- eller rensning af ledig plads-handling) - Denne funktion giver mulighed for at stoppe makulerings- eller rensning af ledig plads-handlingen. Der henvises til Afbrydelse af en makulerings- eller rensning af ledig plads-handling på side 75 for detaljerede oplysninger.
- View the log files (Se logfilerne) - Denne funktion giver mulighed for at få vist logfiler for makulering og rensning af ledig plads, der indeholder eventuelle fejl eller svigt fra den sidste makulerings- eller rensning af ledig plads-handling. Der henvises til Visning af logfilerne på side 75 for detaljerede oplysninger.

BEMÆRK: Makulerings- eller rensning af ledig plads-handlingen kan tage en del tid. Selvom makulering og rensning af ledig plads foregår i baggrunden, kan din computer køre langsommere på grund af den forøgede processoranvendelse.

Brug af en tastesekvens for at starte makulering

Benyt følgende fremgangsmåde for at angive en tastesekvens:

1. Åbn File Sanitizer, og klik på **Shred** (Makuler).
2. Markér afkrydsningsfeltet **Tastesekvens**.
3. Indtast et tegn i tekstboksen
4. Marker enten afkrydsningsfeltet **CTRL** eller afkrydsningsfeltet **ALT**, og marker derefter afkrydsningsfeltet **SHIFT (SKIFT)**.

   Hvis du f.eks. vil starte automatisk makulering vha. s-tasten og Ctrl+Shift, skal du skrive `s` i tekstboksen og derefter markere afkrydningsfelterne **CTRL** og **SHIFT**.

BEMÆRK: Sørg for at vælge en tastesekvens, der er anderledes end andre tastesekvenser, som du har konfigureret.

Sådan starter du makulering vha. en tastesekvens:

1. Hold tasterne shift (Skift) og ctrl eller alt nede (eller den kombination, du har angivet), mens du trykker på det valgte tegn.
2. Klik på **Ja**, hvis der åbnes en bekræftelsesdialogboks.

Brug af ikonet for File Sanitizer

△ **FORSIGTIG:** Makulerede aktiver kan ikke gendannes. Overvej nøje, hvilke elementer du vælger til manuel makulering.

1. Navigér til det dokument eller den mappe, som du vil makulere.
2. Træk aktivet over i ikonet **File Sanitizer** på skrivebordet.
3. Klik på **Ja**, når bekræftelsesdialogboksen åbnes.

Manuel makulering af ét aktiv

△ **FORSIGTIG:** Makulerede aktiver kan ikke gendannes. Overvej nøje, hvilke elementer du vælger til manuel makulering.

1. Højreklik på ikonet for **HP ProtectTools** i meddelelsesområdet længst til højre på proceslinjen, klik på **File Sanitizer**, og klik derefter på **Shred One** (Makulér ét).
2. Når dialogboksen Gennemse åbnes, skal du navigere til det aktiv, som du vil makulere, og derefter klikke på **OK**.

   BEMÆRK: Det valgte aktiv kan være en enkelt fil eller mappe.

3. Klik på **Ja**, når bekræftelsesdialogboksen åbnes.

- eller -

1. Højreklik på ikonet for **File Sanitizer** på skrivebordet, og klik derefter på **Shred One** (Makulér ét).
2. Når dialogboksen Gennemse åbnes, skal du navigere til det aktiv, som du vil makulere, og derefter klikke på **OK**.
3. Klik på **Ja**, når bekræftelsesdialogboksen åbnes.

- eller -

1. Åbn File Sanitizer, og klik på **Shred** (Makuler).
2. Klik på knappen **Gennemse**.
3. Når dialogboksen Gennemse åbnes, skal du navigere til det aktiv, som du vil makulere, og derefter klikke på **OK**.
4. Klik på **Ja**, når bekræftelsesdialogboksen åbnes.

Manuel makulering af alle valgte elementer

1. Højreklik på ikonet for **HP ProtectTools** i meddelelsesområdet længst til højre på proceslinjen, klik på **File Sanitizer**, og klik derefter på **Shred Now** (Makulér nu).
2. Klik på **Ja**, når bekræftelsesdialogboksen åbnes.

- eller -

1. Højreklik på ikonet for **File Sanitizer** på skrivebordet, og klik derefter på **Shred Now** (Makulér nu).
2. Klik på **Ja**, når bekræftelsesdialogboksen åbnes.

- eller -

1. Åbn File Sanitizer, og klik på **Shred** (Makuler).
2. Klik på knappen **Shred Now** (Makuler nu).
3. Klik på **Ja**, når bekræftelsesdialogboksen åbnes.

Manuel aktivering af rensning af ledig plads

1. Højreklik på ikonet for **HP ProtectTools** i meddelelsesområdet længst til højre på proceslinjen, klik på **File Sanitizer**, og klik derefter på **Bleach Now** (Rens nu).
2. Klik på **Ja**, når bekræftelsesdialogboksen åbnes.

- eller -

1. Åbn File Sanitizer, og klik på **Free Space Bleaching** (Fri plads til rensning).
2. Klik på **Bleach Now** (Rens nu).
3. Klik på **Ja**, når bekræftelsesdialogboksen åbnes.

Afbrydelse af en makulerings- eller rensning af ledig plads-handling

Når en makulerings- eller rensning af ledig plads-handling er i gang, vises der en meddelelse over ikonet for HP ProtectTools Security Manager i meddelelsesområdet. Meddelelsen indeholder detaljer vedrørende makuleringen eller rensningen af ledig plads (procent færdiggjort) og giver mulighed for at afbryde handlingen.

Sådan afbrydes handlingen:

▲ Klik på meddelelsen, og klik derefter på **Stop** for at annullere handlingen.

Visning af logfilerne

Hver gang en makulerings- eller rensning af ledig plads-handling udføres, genereres der logfiler over eventuelle fejl eller svigt. Logfilerne er altid opdateret i henhold til den seneste makulerings- eller rensning af ledig plads-handling.

BEMÆRK: Filer, som det lykkes at makulere eller rense, vises ikke i logfilerne.

Der oprettes én logfil for makuleringshandlinger, og en anden logfil oprettes for rensning af ledig plads-handlinger. Begge logfiler findes på harddisken:

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

11 Device Access Manager til HP ProtectTools (kun udvalgte modeller)

Administratorer af Windows®-operativsystemet anvender Device Access Manager for HP ProtectTools til at styre adgang til enhederne på et system og til at beskytte mod uautoriseret adgang:

- Enhedsprofiler oprettes for hver bruger for at definere de enheder, som de har tilladelse til eller nægtet tilladelse til at få adgang til.
- Brugerne er også organiseret i grupper, som f.eks. de foruddefinerede grupper til Device Administrator (Enhedsadministrator). Grupper kan også defineres ved hjælp af muligheden Computeradministration i sektionen Administration på Kontrolpanelet.
- Enhedsadgang kan gives eller nægtes på grundlag af gruppemedlemskab.
- For enhedsklasser, som f.eks. cd-rom-drev og dvd-drev, kan der tillades eller nægtes separat læse- og skriveadgang.

Begrænsede brugere kan også få tilladelse til at læse og ændre politikken til enhedsadgangsstyring.

Opsætningsprocedurer

Åbn Device Access Manager

Følg disse trin for at åbne Device Access Manager:

1. Klik på **Start**, klik på **Alle programmer**, klik på **HP** og klik derefter på **HP ProtectTools Administrative Console**.
2. Klik på **Device Access Manager** i venstre rude.

Konfiguration af enhedsadgang

Device Access Manager til HP ProtectTools har tre visninger:

- Visningen Simple Configuration (Simpel konfiguration) anvendes til at give eller nægte adgang til enhedsklasser for medlemmer af gruppen Device Administrators (Enhedsadministratorer).
- Visningen Device Class Configuration (Konfiguration af enhedsklasse) anvendes til at give eller nægte adgang til enhedstyper eller specifikke enheder for specifikke brugere eller grupper.
- Visningen User Access Settings (Brugeradgangsindstillinger) anvendes til at angive, hvilke brugere der kan få vist eller redigere oplysninger om Simple Configuration (Simpel konfiguration) og Device Class Configuration (Konfiguration af enhedsklasse).

Gruppen Device administrators (Enhedsadministratorer)

Når Device Access Manager installeres, oprettes en gruppe for Device Administrators (Enhedsadministratorer).

Systemadministratoren kan implementere en politik for simpel enhedsadgangsstyring ved at nægte adgang til et sæt af enhedsklasser, medmindre en bruger er klassificeret som en, man har tillid til (vedrørende enhedsadgang). Den anbefalede måde til at skelne mellem "enhedsbetroede" brugere og "ikke enhedsbetroede" brugere er at gøre alle "enhedsbetroede" brugere til medlem af gruppen Device Administrators (Enhedsadministratorer). Ved at give medlemmer af gruppen Device Administrators (Enhedsadministratorer) adgang til enheder via visninger i Simple Configuration (Simpel konfiguration) eller i Device Class Configuration (Enhedsklassekonfiguration) sikres det, at "enhedsbetroede" brugere har fuld adgang til det specificerede sæt af enhedsklasser.

BEMÆRK: Tilføjelse af en bruger til gruppen Device Administrators (Enhedsadministratorer) giver ikke automatisk brugeren tilladelse til at få adgang til enheder. Visningen Simple Configuration (Simpel konfiguration) kan dog anvendes til at give adgang til det krævede sæt af enhedsklasser til "enhedsbetroede" brugere.

Følg nedenstående trin for at tilføje brugere til gruppen Device Administrators (Enhedsadministratorer):

- For Windows 7, Vista eller XP Professional: Brug standard "Lokale brugere og grupper" MMC snap-in.
- For hjemmeversioner af Windows 7, Vista® eller XP: Fra en konto med rettigheder skal du indtaste følgende i et kommando-prompt-vindue:

```
c:\> net localgroup "Enhedsadministratorer"-brugernavn /ADD
```

Simpel konfiguration

Administratorer og autoriserede brugere kan anvende visningen Simple Configuration (Simpel konfiguration) til at få vist eller ændre adgang til følgende enhedsklasser for alle ikke-Device Administrators (Enhedsadministratorer):

BEMÆRK: For at bruge denne visning til at læse oplysninger om enhedsadgang, skal brugeren eller gruppen have "læse"-adgang i visningen **User Access Settings** (Brugeradgangsindstillinger). For at bruge denne visning til at redigere oplysninger om enhedsadgang, skal brugeren eller gruppen have "rette"-adgang i visningen **User Access Settings** (Brugeradgangsindstillinger).

- Alle flytbare medier (disketter, USB-flash-drev osv.)
- Alle dvd/cd-rom-drev
- Alle serielle og parallelle porte
- Alle Bluetooth® -enheder
- Alle infrarøde enheder
- Alle modemenheder
- Alle PCMCIA-enheder
- Alle 1394-enheder

Følg nedenstående trin for at tillade eller nægte adgang til en klasse af enheder for alle, der ikke er Device Administrators (Enhedsadministratorer):

1. I venstre rude skal du klikke på **HP ProtectTools Administrative Console**, klikke på **Device Access Manager** og derefter klikke på **Simple Configuration** (Simpel konfiguration).
2. For at nægte adgang skal du i højre rude markere afkrydsningsfeltet for en enhedsklasse eller en specifik enhed. Fjern markeringen i afkrydsningsfeltet for at give adgang til den pågældende enhedsklasse eller specifikke enhed.

   Hvis afkrydsningsfeltet er nedtonet, er værdier, der har indflydelse på adgangsscenarierne, blevet ændret i visningen Device Class Configuration (Konfiguration af enhedsklasse). Hvis du vil sætte værdierne tilbage til simple indstillinger, skal du fjerne markeringen i afkrydsningsfeltet for at slette eller indstille dem og derefter klikke på **Ja** for at bekræfte.
3. Klik på ikonet for **Gem**.

   BEMÆRK: Hvis tjenester kører i baggrunden, åbnes en dialogboks, der spørger, om du vil starte. Klik på **Ja**.
4. Klik på **OK**.

Start af baggrundstjeneste

Før enhedsprofiler kan anvendes, åbnes en dialogboks til HP ProtectTools Security Manager, der spørger om du vil starte baggrundstjenesten til HP ProtectTools Device Locking/Auditing. Klik på **Ja**. Baggrundstjenesten starter og vil derefter starte automatisk, når systemet starter.

BEMÆRK: Der skal defineres en enhedsprofil, før baggrundstjenestens prompt vises.

Administratorer kan også starte eller stoppe denne tjeneste:

1. Klik på **Start**, og klik derefter på **Kontrolpanel**.
2. Klik på **Administration**, og klik derefter på **Tjenester**.
3. Søg efter tjenesten for **HP ProtectTools Device Locking/Auditing**.

Stop af Device Locking/Auditing-tjenesten stopper ikke låsningen af enheden. To komponenter sikrer låsning af enheden:

- Tjenesten Device Locking/Auditing
- DAMDrv.sys-drevet

Når tjenesten startes, starter enhedsdriveren, men stop af tjenesten stopper ikke driveren.

For at afgøre om baggrundstjenesten kører, skal du åbne et kommando-prompt-vindue og derefter indtaste sc query flcdlock.

For at afgøre om enhedsdriveren kører, skal du åbne et kommando-prompt-vindue, og derefter indtaste sc query damdrv.

Device Class Configuration (Konfiguration af enhedsklasse)

Administratorer og autoriserede brugere kan få vist og ændre lister med brugere og grupper, der ikke har tilladelse eller er nægtet adgang til klasser med enheder eller specifikke enheder.

BEMÆRK: For at bruge denne visning til at læse oplysninger om enhedsadgang, skal brugeren eller gruppen have "læse"-adgang i visningen **User Access Settings** (Brugeradgangsindstillinger). For at bruge denne visning til at redigere oplysninger om enhedsadgang, skal brugeren eller gruppen have "rette"-adgang i visningen **User Access Settings** (Brugeradgangsindstillinger).

Visningen Device Class Configuration (Konfiguration af enhedsklasse) har følgende sektioner:

- **Device List** (Enhedsliste) - Viser alle enhedsklasser og enheder, der er installeret på systemet eller tidligere har været installeret på systemet.
  - Beskyttelse anvendes normalt for en enhedsklasse. En valgt bruger eller gruppe vil kunne få adgang til enhver enhed i enhedsklassen.
  - Beskyttelse kan også gælde for specifikke enheder.
- **User List** (Brugerliste) - Viser alle brugere og grupper, der har tilladelse eller er nægtet adgang til de valgte enhedsklasser eller specifikke enheder.
  - Elementet i brugerlisten kan foretages for en specifik bruger eller for en gruppe, hvoraf brugeren er medlem.
  - Hvis et bruger- eller gruppeelement i brugerlisten ikke er tilgængeligt, er indstillingen arvet fra enhedsklassen i enhedslisten eller fra klassemappen.
  - Nogle enhedsklasser, som f.eks. dvd og cd-rom, kan yderligere styres ved at tillade eller nægte adgang separat for læse- og skrivehandlinger.

    Som for andre enheder og klasser kan læse- og skriveadgangsrettigheder arves. Læseadgang kan f.eks. arves fra en højere klasse, men skriveadgang kan specifikt nægtes for en bruger eller gruppe.

BEMÆRK: Hvis afkrydsningsfeltet for læs er tomt, har adgangskontrolelementet ingen effekt på læseadgang til enheden. Det hverken giver eller nægter læseadgang til enheden.

Eksempel 1 - Hvis en bruger eller gruppe nægtes skriveadgang til en enhed eller klasse af enheder:

Den samme bruger, den samme gruppe eller medlem af samme gruppe kan kun få skriveadgang eller læse-/skriveadgang til en enhed under denne enhed i enhedshierarkiet.

Eksempel 2 - Hvis en bruger eller gruppe har skriveadgang til en enhed eller klasse af enheder:

Den samme bruger, den samme gruppe eller medlem af samme gruppe kan kun blive nægtet skriveadgang eller læse-/skriveadgang til den samme enhed eller en enhed under denne enhed i enhedshierarkiet.

Eksempel 3 - Hvis en bruger eller gruppe har læseadgang til en enhed eller klasse af enheder:

Den samme bruger, den samme gruppe eller medlem af samme gruppe kan kun blive nægtet læseadgang eller læse-/skriveadgang til den samme enhed eller en enhed under denne enhed i enhedshierarkiet.

Eksempel 4 - Hvis en bruger eller gruppe er nægtet læseadgang til en enhed eller klasse af enheder:

Den samme bruger, den samme gruppe eller medlem af samme gruppe kan kun få læseadgang eller læse-/skriveadgang til en enhed under denne enhed i enhedshierarkiet.

Eksempel 5 - Hvis en bruger eller gruppe har læse-/skriveadgang til en enhed eller klasse af enheder:

Den samme bruger, den samme gruppe eller medlem af samme gruppe kan kun blive nægtet skriveadgang eller læse-/skriveadgang til den samme enhed eller en enhed under denne enhed i enhedshierarkiet.

Eksempel 6 - Hvis en bruger eller gruppe er nægtet læse-/skriveadgang til en enhed eller klasse af enheder:

Den samme bruger, den samme gruppe eller medlem af samme gruppe kan kun få læseadgang eller læse-/skriveadgang til en enhed under denne enhed i enhedshierarkiet.

Nægtelse af adgang til en bruger eller gruppe

Følg nedenstående trin for at forhindre en gruppe i af få adgang til en enhed eller en klasse af enheder:

1. I venstre rude skal du klikke på **HP ProtectTools Administrative Console**, klikke på **Device Access Manager** og derefter klikke på **Device Class Configuration** (Konfiguration af enhedsklasse).
2. Klik på den enhedsklasse, du vil konfigurere i enhedslisten.
   - Enhedsklasse
   - Alle enheder
   - Individuel enhed
3. Under **User/Groups** (Bruger/grupper) skal du klikke på den bruger eller gruppe, der skal nægtes adgang.

4. Klik på **Nægt** ud for en bruger eller gruppe.
5. Klik på ikonet for **Gem**.

BEMÆRK: Når indstillinger for nægtelse og tilladelse er angivet på samme enhedsniveau for en bruger, har nægtelse fortrin for tilladelse af adgang.

Tilladelse af adgang for en bruger eller en gruppe

Følg nedenstående trin for at give en bruger eller en gruppe adgang til en enhed eller en klasse af enheder:

1. I venstre rude skal du klikke på **HP ProtectTools Administrative Console**, klikke på **Device Access Manager** og derefter klikke på **Device Class Configuration** (Konfiguration af enhedsklasse).
2. I enhedslisten skal du klikke på ét af følgende:
   - Enhedsklasse
   - Alle enheder
   - Individuel enhed
3. Klik på **Tilføj**.

   Dialogboksen **Select Users or Groups** (Vælg bruger eller grupper) åbnes.
4. Klik på **Advanced** (Avanceret), og klik derefter på **Find Now** (Find nu) for at søge efter brugere eller grupper, der skal tilføjes.
5. Klik på en bruger eller en gruppe, der skal føjes til listen med tilgængelige brugere og grupper, og klik derefter på **OK**.
6. Klik på **OK** igen.
7. Klik på **Tillad** for at give denne bruger eller gruppe adgang.
8. Klik på ikonet for **Gem**.

Fjernelse af adgang for en bruger eller en gruppe

Følg nedenstående trin for at fjerne tilladelse for en bruger eller en gruppe til at få adgang til en enhed eller en klasse af enheder:

1. I venstre rude skal du klikke på **HP ProtectTools Administrative Console**, klikke på **Device Access Manager** og derefter klikke på **Device Class Configuration** (Konfiguration af enhedsklasse).
2. Klik på den enhedsklasse, du vil konfigurere i enhedslisten.
   - Enhedsklasse
   - Alle enheder
   - Individuel enhed

3. Under **User/Groups** (Bruger/gruppe) skal du klikke på den bruger eller gruppe, du vil fjerne, og derefter klikke på **Fjern**.

4. Klik på ikonet for **Gem**.

Tilladelse af adgang til en klasse af enheder for én bruger i en gruppe

Følg nedenstående trin for at tillade en bruger at få adgang til en klasse af enheder, og samtidig nægte adgang til andre medlemmer af den pågældende brugergruppe:

1. I venstre rude skal du klikke på **HP ProtectTools Administrative Console**, klikke på **Device Access Manager** og derefter klikke på **Device Class Configuration** (Konfiguration af enhedsklasse).

2. Klik på den enhedsklasse, du vil konfigurere i enhedslisten.

   - Enhedsklasse
   - Alle enheder
   - Individuel enhed

3. Under **User/Groups** (Bruger/grupper) skal du vælge den gruppe, der skal nægtes adgang, og derefter klikke på **Nægt**.

4. Naviger til den mappe, der ligger under mappen for den påkrævede klasse, og tilføj derefter den bestemte bruger.

5. Klik på **Tillad** for at give denne bruger adgang.

6. Klik på ikonet for **Gem**.

Tilladelse af adgang til en bestemt enhed for én bruger i en gruppe

Administratorer kan give en bruger adgang til en bestemt enhed og samtidig nægte adgang til alle andre medlemmer af den brugers gruppe for alle enheder i klassen:

1. I venstre rude skal du klikke på **HP ProtectTools Administrative Console**, klikke på **Device Access Manager** og derefter klikke på **Device Class Configuration** (Konfiguration af enhedsklasse).

2. I enhedslisten klikker du på den enhedsklasse, som du vil konfigurere, og dernæst navigerer du til mappen under den.

3. Klik på **Add** (Tilføj). Dialogboksen **Select Users or Groups** (Vælg bruger eller grupper) åbnes.

4. Klik på **Advanced** (Avanceret), og klik derefter på **Find Now** (Find nu) for at søge efter brugerens gruppe, der skal nægtes adgang til alle enheder i klassen.

5. Klik på gruppen, og klik derefter på **OK**.

6. Naviger til den bestemte enhed under enhedsklassen, hvortil brugeren skal have adgang.

7. Klik på **Add** (Tilføj). Dialogboksen **Select Users or Groups** (Vælg bruger eller grupper) åbnes.

8. Klik på **Advanced** (Avanceret), og klik derefter på **Find Now** (Find nu) for at søge efter brugere eller grupper, der skal tilføjes.

9. Klik på den bruger, der skal have adgang, og klik derefter på **OK**.

10. Klik på **Tillad** for at give denne bruger adgang.
11. Klik på ikonet for **Gem**.

Nulstilling af konfigurationen

△ **FORSIGTIG:** Nulstilling af konfigurationen frasorterer alle enhedskonfigurationsændringer, der er blevet foretaget og alle indstillinger vender tilbage til standardindstillingen.

Følg nedenstående trin for at nulstille konfigurationsindstillingerne til standardværdier:

1. I venstre rude skal du klikke på **HP ProtectTools Administrative Console**, klikke på **Device Access Manager** og derefter klikke på **Device Class Configuration** (Konfiguration af enhedsklasse).
2. Klik på knappen **Reset** (Nulstil).
3. Klik på **Ja** for at bekræfte.
4. Klik på ikonet for **Gem**.

Avancerede opgaver

Kontrol af adgang til konfigurationsindstillingerne

I visningen **User Access Settings** (Brugeradgangsindstillinger) angiver administratorerne de grupper eller brugere, der har tilladelse til at anvende siderne Simple Configuration (Simpel konfiguration) og Device Class Configuration (Konfiguration af enhedsklasse).

BEMÆRK: En bruger eller gruppe skal have "Fulde brugeradministratorrettigheder" for at ændre indstillingerne i visningen User Access Settings (Brugeradgangsindstillinger).

- En bruger eller gruppe skal have "Vis (skrivebeskyttet) konfigurationsindstillinger"-adgang i visningen User Access Settings (Brugeradgangsindstillinger) for at få vist oplysningerne i Simple Configuration (Simpel konfiguration) og (Konfiguration af enhedsklasse).
- En bruger eller gruppe skal have "Ændr konfigurationsindstillinger"-adgang i visningen User Access Settings (Brugeradgangsindstillinger) for at ændre oplysningerne i Simple Configuration (Simpel konfiguration) og Device Class Configuration (Konfiguration af enhedsklasse).

BEMÆRK: Selv medlemmer af gruppen Administrator skal have "læse"-adgang for at få vist Simple Configuration (Simpel konfiguration) og (Konfiguration af enhedsklasse) og have "rette"-adgang for at ændre data vha. visningerne Simple Configuration (Simpel konfiguration) og Device Class Configuration (Konfiguration af enhedsklasse).

BEMÆRK: Efter evaluering af adgangsniveauerne for alle brugere og grupper, og hvis en bruger ikke har valgt hverken Tillad eller Nægt for et bestemt adgangsniveau, nægtes brugeren adgang på dette niveau.

Give adgang til en eksisterende gruppe eller bruger

Følg nedenstående trin for at give tilladelse til en eksisterende gruppe eller bruger til at få vist eller ændre konfigurationsindstillingerne:

1. I venstre rude skal du klikke på **HP ProtectTools Administrative Console**, klikke på **Device Access Manager** og derefter klikke på **User Access Settings** (Brugeradgangsindstillinger).
2. Klik på en gruppe eller bruger for at give adgang.
3. Under **Tilladelser** skal du klikke på **Tillad** for hver type af tilladelse der gives til den valgte gruppe eller bruger.

   BEMÆRK: De givne tilladelser kan akkumuleres. F.eks. får en bruger, der har fået "Ændr konfigurationsindstillinger", automatisk "Vis (læseadgang) konfigurationsindstillinger"-tilladelse. En bruger, som har fået "Fulde brugeradministratorrettigheder", får også "Ændr konfigurationsindstillinger" og "Vis (læseadgang) konfigurationsindstillinger"-adgang.

   - Fulde brugeradministratorrettigheder
   - Ændr konfigurationsindstillinger
   - Vis (læseadgang) konfigurationsindstillinger
4. Klik på ikonet for **Gem**.

Nægte adgang til en eksisterende gruppe eller bruger

Følg nedenstående trin for at nægte tilladelse for en eksisterende gruppe eller bruger til at få vist eller ændre konfigurationsindstillingerne:

1. I venstre rude skal du klikke på **HP ProtectTools Administrative Console**, klikke på **Device Access Manager** og derefter klikke på **User Access Settings** (Brugeradgangsindstillinger).
2. Klik på en gruppe eller bruger, der nægtes adgang.
3. Under **Tilladelser** skal du klikke på **Nægt** for hver type af tilladelse der nægtes til den valgte gruppe eller bruger:
   - Fulde brugeradministratorrettigheder
   - Ændr konfigurationsindstillinger
   - Vis (læseadgang) konfigurationsindstillinger
4. Klik på ikonet for **Gem**.

Tilføjelse af en ny gruppe eller bruger

Følg nedenstående trin for at give tilladelse for en eksisterende gruppe eller bruger til at få vist eller ændre konfigurationsindstillingerne:

1. I venstre rude skal du klikke på **HP ProtectTools Administrative Console**, klikke på **Device Access Manager** og derefter klikke på **User Access Settings** (Brugeradgangsindstillinger).
2. Klik på **Add** (Tilføj). Dialogboksen **Select Users or Groups** (Vælg bruger eller grupper) åbnes.
3. Klik på **Advanced** (Avanceret), og klik derefter på **Find Now** (Find nu) for at søge efter brugere eller grupper, der skal tilføjes.
4. Klik på en gruppe eller bruger, klik på **OK**, og klik derefter på **OK** igen.
5. Klik på **Tillad** for at give denne bruger adgang.
6. Klik på ikonet for **Gem**.

Fjernelse af gruppe- eller brugeradgang

Følg nedenstående trin for at fjerne tilladelse for en gruppe eller bruger til at få vist eller ændre konfigurationsindstillingerne:

1. I venstre rude skal du klikke på **HP ProtectTools Administrative Console**, klikke på **Device Access Manager** og derefter klikke på **User Access Settings** (Brugeradgangsindstillinger).
2. Klik på en gruppe, og klik derefter på **Fjern**.
3. Klik på ikonet for **Gem**.

Relateret dokumentation

Device Access Manager til HP ProtectTools er kompatibel med virksomhedsproduktet HP ProtectTools Enterprise Device Access Manager. Når du arbejder med virksomhedsproduktet, giver Device Access Manager til HP ProtectTools læseadgang til dets egne funktioner.

Der findes flere oplysninger om Device Access Manager til HP ProtectTools på internettet på adressen http://www.hp.com/hps/security/products.

12 LoJack Pro til HP ProtectTools

Med Absolute Softwares linje af Computrace-produkter kan brugerne spore deres HP-computere og øge databeskyttelsen. Computrace LoJack-produkterne reducerer også maskinfald og hjælper med at genfinde stjålne maskiner.

Følg disse instruktioner for at aktivere Computrace-produktet:

1. Klik på **Start**, klik på **Alle programmer**, og klik derefter på **HP ProtectTools Security Manager**.
2. Klik på **Theft Recovery**, og klik derefter på **Activate Now** (Aktiver nu).

   Din standardwebbrowser åbner et abonnementwebside, hvor du kan vælge og købe et af de tre Computrace-produkter, der er tilgængelig med HP ProtectTools:

   - **Computrace Data Delete** - Omfatter fjernsletning af data, fastfrysning af enheder og grundlæggende sporing og rapportering af aktiver.
   - **Computrace LoJack Pro** - Omfatter fjernsletning af data, fastfrysning af enheder, grundlæggende sporing og rapportering af aktiver samt styring af genfundent tyverigods.
   - **Computrace LoJack Pro Premium** - Omfatter fjernsletning af data, fastfrysning af enheder, avanceret sporing og rapportering af aktiver, geolokalisering og geofencing (markering af elektronisk hegn) samt styring af genfundent tyverigods.

Computrace Agent er integreret i BIOS på HPs bærbare computere, også selv om Agent er slukket, når computeren skal leveres. Når du har købt dit abonnement, kan Agent aktiveres. Det integrerede Agent kan geninstallere operativsystemet og omformatere harddiske.

BEMÆRK: Abonnementsperioder kan fås fra 1-5 år. Der henvises til Absolute Software's abonnementsaftale angående yderligere detaljer. Gendannelsesfunktionen afhænger af den geografiske placering. GPS-sporing understøttes på udvalgte modeller med WWAN-funktion.

13 Fejlfinding

HP ProtectTools Security Manager

Kort beskrivelse	Detaljer	Løsning
Chipkort og USB-tokens er ikke tilgængelige i Security Manager, hvis de er installeret, efter at Security Manager er installeret.	For at kunne bruge chipkort eller USB-tokens i Security Manager skal den understøttende software (drivere, PKCS#11-leverandører osv.) installeres forud for installation af Security Manager. Hvis Security Manager allerede er installeret, skal du benytte følgende fremgangsmåde, efter at du har installeret chipkort- eller tokenunderstøttet software:	Log ind på Password Manager. I HP ProtectTools Security Manager skal du klikke på **Password Manager**, klikke på **Credentials** (Legitimationsoplysninger) og derefter klikke på **Smart Card** (Chipkort) Genstart computeren, hvis du bliver bedt om det.
Nogle programwebsider opretter fejl, der forhindrer brugeren i at udføre eller fuldføre opgaver.	Nogle webbaserede programmer holder op med at fungere og rapporterer fejl på grund af funktionsmønsteret ved deaktivering af Enkelt sign-on. Et **!** i en gul trekant kan f.eks. ses i Internet Explorer og angiver, at der er opstået en fejl.	Security Manager Single Sign On understøtter ikke alle websoftwaregrænseflader. Deaktivér Single Sign On-understøttelse for den bestemte webside ved at slå Single Sign On-understøttelse fra. Se fuldstændig dokumentation vedrørende Single Sign On, som er tilgængelig i hjælpefilerne i programmet Security Manager. Hvis et specifikt Enkelt sign-on ikke kan deaktiveres for et bestemt program, kan du kontakte HP Teknisk support og anmode om support på tredje niveau via din HP Service-kontaktperson.
Indstillingen **Søg efter virtuelt token** vises ikke under logon.	Brugeren kan ikke flytte placeringen af en registreret virtuel token i Password Manager, da indstillingen til at gennemse blev fjernet for at reducere sikkerhedsrisici.	Søgeindstillingen er blevet fjernet, fordi den gjorde det muligt for ikke-brugere at slette og omdøbe filer og tage styring over Windows.
Domæneadministratorer kan ikke ændre Windows-adgangskoder, heller ikke med autorisation.	Dette sker, når en domæneadministrator logger på et domæne og registrerer domæneidentiteten sammen med Password Manager ved hjælp af administratorens rettigheder på domænet og den lokale pc. Når domæneadministratoren forsøger at ændre Windows-adgangskoden fra Password Manager, få administratoren en fejlmeddelelse ved logon: **Begrænsning af brugerkonto**.	Password Manager kan ikke ændre en domænebrugers kontoadgangskode via **Change Windows password** (Skift logon-adgangskode til Windows). Security Manager kan kun ændre de lokale pc-kontoadgangskoder. Domænebrugeren kan ændre sin adgangskode via indstillingen **Change password** (Skift adgangskode) i **Windows security** (Windows-sikkerhed), men eftersom domænebrugeren ikke har en fysisk konto på den lokale pc, kan Password Manager kun ændre den adgangskode, der anvendes til at logge på.
Password Manager har inkompatibilitetsproblemer med Corel WordPerfect 12 adgangskode GINA.	Hvis brugeren logger på Password Manager, opretter et dokument i WordPerfect og gemmer det med adgangskodebeskyttelse, kan Password	HP arbejder på at udvikle en løsning til fremtidige produktforbedringer.

Kort beskrivelse	Detaljer	Løsning
	Manager, hverken manuelt eller automatisk, registrere eller genkende adgangskoden GINA.	
Password Manager genkender ikke knappen **Connect** (Opret forbindelse).	Hvis Enkelt sign-on-legitimationsoplysningerne til RDP (Remote Desktop Connection) angives til **Connect** (Tilslut), når Enkelt sign-on startes igen, angives **Save As** (Gem som) altid i stedet for **Connect** (Tilslut).	HP arbejder på at udvikle en løsning til fremtidige produktforbedringer.
Brugeren kan ikke logge på Password Manager efter overgang fra Standby- til Dvaletilstand, men kun på Windows XP Service Pack 1.	Når systemet overgår til dvale- eller slumretilstand, kan administratoren eller brugeren ikke logge på Password Manager, og Windows-logonskærmen vises fortsat, uanset, hvilke legitimationsoplysninger (adgangskode, fingeraftryk eller Java Card), der vælges.	Opdatér Windows til Service Pack 2 via Windows Update. Se i Microsoft Knowledge Base artikel 813301 på adressen http://www.microsoft.com for yderligere oplysninger om årsagen til problemet. For at logge på skal brugeren vælge Password Manager og derefter logge på. Når der er logget på Password Manager, bliver brugeren bedt om at logge på Windows (brugeren skal vælge Windows-logonindstillingen) for at afslutte logonprocessen. Hvis brugeren først logger på Windows, skal brugeren derefter manuelt logge på Password Manager.
Sikkerhedsprocessen **Restore Identity** (Gendan identitet) mister tilknytningen til det virtuelle token.	Når brugeren gendanner identitet, kan Password Manager miste tilknytningen til placeringen af det virtuelle token på logonskærmbilledet. Selv om Password Manager har registreret det virtuelle token, skal brugeren registrere token for at gendanne tilknytningen.	Dette er standard på nuværende tidspunkt. Ved afinstallation af Security Manager, uden at beholde identiteter, tilintetgøres systemdelen (server) af token, så denne ikke kan anvendes mere til at logge på, selv om klientdelen af token gendannes via gendannelse af identitet. HP arbejder på langsigtede løsninger.

Device Access Manager til HP ProtectTools

Brugerne er blevet nægtet adgang til enheder i Device Access Manager, men der er fortsat ikke adgang til enhederne.

- **Forklaring** - Simple Configuration (Simpel konfiguration) og/eller Device Class Configuration (Konfiguration af enhedsklasse) er blevet anvendt i Device Access Manager til at nægte brugere adgang til enhederne. Selv om brugerne nægtes adgang, kan de fortsat få adgang til enhederne.
- **Løsning:**
  - Kontrollér, om HP ProtectTools Device Locking-tjenesten er startet.
  - Som en administrativ bruger skal du klikke på **Kontrolpanel**, og derefter klikke på **System og vedligeholdelse**. I vinduet Administration skal du klikke på **Tjenester** og søge efter tjenesten **HP ProtectTools Device Locking/Auditing** Kontrollér, at tjenesten er startet, og at den angivne opstartstype er **Automatisk**

En bruger har uventet adgang til en enhed, eller en bruger er uventet nægtet adgang til en enhed.

- **Forklaring** - Device Access Manager har været anvendt til at nægte brugere adgang til nogle enheder og tilladt brugere adgang til andre enheder. Når brugeren anvender systemet, kan denne få adgang til enheder, som denne tror, at Device Access Manager har nægtet adgang til, og bliver nægtet adgang til enheder, som denne tror Device Access Manager bør tillade.
- **Løsning:**
  - Brug Device Class Configuration (Konfiguration af enhedsklasse) i Device Access Manager for at undersøge brugerens enhedsindstillinger.
  - Klik på **Security Manager**, klik på **Device Access Manager**, og klik derefter på **Device Class Configuration**. Udvid niveauerne i træet Device Class (Enhedsklasse), og gennemse de indstillinger, der er relevante for brugeren. Se, om der forekommer "Nægt"-tilladelser, der kan være angivet for brugeren eller nogen Windows-gruppe, som de kan være medlem af, f.eks. Brugere, Administratorer.

Tillad eller nægt - hvilken har fortrin?

- **Forklaring** – I Device Class Configuration (Konfiguration af enhedsklasse) er følgende konfiguration indstillet:
  - Tilladelsen Tillad er blevet givet til en Windows-gruppe (f.eks. BUILTIN\Administratorer) og tilladelsen Nægt er blevet givet til en anden Windows-gruppe (f.eks. BUILTIN\Users) på samme niveau i klassehierarkiet for enheden (f.eks. dvd/cd-rom-drev).
  - Hvis en bruger er medlem af begge grupper (f.eks. Administrator) - hvilken har fortrin?
- **Løsning:**
  - Brugeren er nægtet adgang til enheden. Nægtelse har fortrin fremfor Tilladelse.
  - Adgang nægtes pga. den måde, som Windows udarbejder de effektive tilladelser for enheden. Én gruppe er nægtet adgang, og én gruppe har fået tilladelse, men brugeren er medlem af begge grupper. Brugeren er nægtet adgang, fordi nægtet-adgang har fortrin fremfor tilladt-adgang.

- Én måde at løse problemet er at nægte gruppen Brugere på dvd/cd-rom-drevniveau adgang og at give gruppen Administratorer på niveauet under dvd/cd-rom-drev adgang.
- En alternativ måde at løse problemet på, er at oprette specifikke Windows-grupper, én med adgang til dvd/cd og én med nægtet adgang til dvd/cd. Bestemte brugere bør derefter tilføjes til den relevante gruppe.

Visningen Simple Configuration (Simpel konfiguration) er blevet anvendt til at definere en politik for simpel enhedsadgangsstyring, men administrative brugere kan ikke få adgang til enhederne.

- **Forklaring** - Simple Configuration (Simpel konfiguration) nægter adgang til Brugere og Gæster, og giver Enhedsadministratorer tilladelse.
- **Løsning:** Tilføj den administrative bruger til gruppen Enhedsadministratorer.

Diverse

Berørt software – kort beskrivelse	Detaljer	Løsning
Security Manager — modtaget advarsel: **The security application can not be installed until the HP Protect Tools Security Manager is installed** (Sikkerhedsprogrammet kan ikke installeres, før HP Protect Tools Security Manager er installeret).	Alle sikkerhedsprogrammer, som f.eks. Java Card Security og biometrik er plug-ins, der kan udvides til Security Manager-brugergrænsefladen. Security Manager skal installeres, før en HP-godkendt sikkerheds-plug-in kan indlæses.	Security Manager-softwaren skal installeres, før en ny sikkerheds-plug-in kan installeres.
HP ProtectTools Security Manager — Der returneres en forbigående fejl, når Security Manager-grænsefladen lukkes.	Der opstår en forbigående fejl (1 ud af 12 tilfælde), når lukknappen øverst til højre på skærmen bruges til at lukke Security Manager, før alle plug-in-programmer er færdige med at blive indlæst.	Dette er relateret til en timing-afhængighed ved plug-in-tjenesters indlæsningstid, når Security Manager lukkes og genstartes. Eftersom PTHOST.exe er shell-programmet for de andre programmer (plug-ins), er det afhængigt af plug-in'en for at kunne udføre indlæsningstiden (tjenester). Lukning af shell-programmet, før plug-in'en har fuldført indlæsningen, er hovedårsagen. Giv Security Manager mulighed for at udføre tjenesteindlæsningsmeddelelsen (vises øverst i Security Manager-vinduet) og alle plug-ins, der vises i venstre kolonne. Undgå fejl ved at give disse plug-ins tid til at indlæses.
HP ProtectTools — Ubegrænset adgang eller ubegrænsede administratorrettigheder udgør en sikkerhedsrisiko.	Mange forskellige risici er mulige i forbindelse med ubegrænset adgang til klient-pc'en, herunder følgende: • Sletning af PSD • Skadelige ændringer af brugerindstillinger • Deaktivering af sikkerhedspolitikker og funktioner	Administratorer opfordres til at følge "bedst praksis" ved begrænsning af privilegier til slutbrugere og begrænsning af brugeradgang. Der bør ikke gives administrative privilegier til uautoriserede brugere.

Ordliste

adgangskode for tilbagekaldelse Adgangskode, som oprettes, når en bruger anmoder om et digitalt certifikat. Adgangskoden kræves, når brugeren ønsker at tilbagekalde sit digitale certifikat. På denne måde sikres det, at kun brugeren kan tilbagekalde certifikatet.

administrator *Se* Windows-administrator.

afsender, der er tillid til En kontaktperson, der er tillid til, som sender signerede og/eller krypterede e-mails og Microsoft Office-dokumenter.

aktiv En datakomponent bestående af personlige oplysninger eller filer, historiske og webrelaterede data osv., som findes på harddisken.

aktivering Den handling, der skal udføres, før funktionerne i Drevkryptering er tilgængelige. Drevkryptering aktiveres vha. guiden Installation HP ProtectTools Setup Wizard. Det er kun administratorer, der kan aktivere Drevkryptering. Aktiveringsprocessen består af aktivering af softwaren, kryptering af drevet, oprettelse af en brugerkonto samt oprettelse af den indledende krypteringsnøgle for sikkerhedskopiering på en flytbar lagerenhed.

ATM Automatic Technology Manager, som gør det muligt for netværksadministratorer at fjernadministrere systemer på BIOS-niveau.

automatisk makulering Planlagt makulering, som brugeren angiver i File Sanitizer.

autoriseret bruger En bruger, der har fået tilladelse af visningen User Access Settings (Brugeradgangsindstillinger) til at få vist eller redigere konfigurationsindstillingerne på visningerne i Simple Configuration (Simpel konfiguration) eller i Device Class Configuration (Konfiguration af enhedsklasse).

baggrundstjeneste Baggrundstjenesten til HP ProtectTools Device Locking/Auditing, der skal køres for at politikker for enhedsadgangsstyring anvendes. Dette kan ses fra programmet Tjenester under indstillingen Administration i Kontrolpanel. Hvis det ikke kører, forsøger HP ProtectTools Security Manager at starte det, når politikker for enhedsadgangsstyring anvendes.

biometrisk Kategori for godkendelsesoplysninger, der bruger et fysisk træk, f.eks. fingeraftryk, til at identificere en bruger.

bruger Enhver, som er tilmeldt i Drive Encryption. Ikke-administratorbrugere har begrænsede rettigheder i Drive Encryption. De kan kun tilmelde sig (med administratorgodkendelse) og logge på.

certificeringsmyndighed Service, som udsteder beviser, der kræves til at køre en offentlig nøgleinfrastruktur.

chathistoriksession En krypteret fil, som indeholder en optegnelse over begge parter i en samtale i en chatsession.

chipkort Lille hardwareenhed på samme størrelse og af samme form som et kreditkort, der lagrer identifikationsoplysninger om ejeren. Bruges til at godkende ejeren af en computer.

cryptographic service provider (CSP) (kryptografisk tjenesteudbyder) Udbyder af eller bibliotek med kryptografiske algoritmer, der kan bruges i en veldefineret grænseflade til at udføre bestemte kryptografiske funktioner.

dekryptering Procedure, der bruges i kryptografi til at konvertere krypterede data til almindelig tekst.

digital signatur Data, som sendes med en fil og verificerer afsenderen af materialet, og at filen ikke er blevet ændret, efter at den blev signeret.

digitalt certifikat Elektroniske kreditiver, som bekræfter en persons eller et firmas identitet ved at knytte ejeren af det digitale certifikats identitet til et sæt elektroniske nøgler, som anvendes til at signere digitale oplysninger.

domæne Gruppe af computere, som er del af et netværk og deler en fælles biblioteksdatabase. Domæner navngives entydigt, og hvert domæne har et sæt almindelige regler og procedurer.

Drevkryptering Beskytter dine data ved at kryptere din/dine harddisk(e), hvilket gør oplysningerne ulæsbare for dem uden korrekt tilladelse.

Drive Encryption-logonskærm (Logonskærm for Drevkryptering) Logonskærm, som vises, før Windows starter. Brugere skal indtaste deres Windows-brugernavn og -adgangskode eller Java Card-PIN-kode. I de fleste tilfælde giver angivelse af de korrekte oplysninger på Drive Encryption-logonskærmen direkte adgang til Windows uden at skulle logge på igen på Windows-logonskærmen.

DriveLock. Sikkerhedsfunktion, som sammenkæder harddisken med en bruger og kræver, at brugeren angiver DriveLock-adgangskoden korrekt, når computeren starter.

Encryption File System (EFS) (Krypteringsfilsystem) System, der krypterer alle filer og undermapper i den valgte mappe.

enhedsklasse Alle enheder af en bestemt type, som f.eks. drev.

fingeraftryk En digital kopi af dit fingeraftryksbillede. Dit faktiske fingeraftryksbillede gemmes aldrig af Security Manager.

foreslået underskriver En bruger, som er udpeget af ejeren af et Microsoft Word- eller Microsoft Excel-dokument til at tilføje en signaturlinje til dokumentet.

forsegling til kontaktpersoner, der er tillid til En handling, som tilføjer en digital signatur, krypterer e-mail'en og sender den, efter at du har godkendt vha. din valgte sikkerhedslogonmetode.

gendanne En proces, der kopierer programoplysninger fra en tidligere, gemt sikkerhedskopifil til dette program.

genstart Processen med at genstarte computeren.

godkendelse Processen med verificering af, hvorvidt en bruger har autorisation til at udføre en opgave, som f.eks. åbne en computer, ændre indstillinger for et bestemt program eller få vist sikrede data.

godkendelse ved start Sikkerhedsfunktion, der kræver en form for godkendelse, f.eks. et Java Card, en sikkerhedschip eller adgangskode, når computeren tændes.

gruppe En gruppe af brugere, der har samme niveau for adgang eller nægtelse til en enhedsklasse eller en bestemt enhed.

HP SpareKey Sikkerhedskopi af drevkrypteringsnøgle.

identitet I Security Manager til HP ProtectTools er det en gruppe legitimationsoplysninger og indstillinger, der håndteres som en konto eller profil for en bestemt bruger.

Id-kort En Windows sidebjælke-gadget, der tjener som visuel identitet for din stationære pc med dit brugernavn og det valgte billede. Klik på Id-kort for at åben HP ProtectTools Administrative Console.

IM-kommunikation, der er tillid til En kommunikationssession, under hvilken betroede meddelelser sendes fra en betroet afsender til en kontaktperson, der er tillid til.

Java Card Et flytbart kort, som indsættes i computeren. Det indeholder identifikationsoplysninger til logon. Hvis du logger på med et Java Card i Drive Encryption-logonskærmen, kræves det, at du indsætter dit Java Card og indtaster dit brugernavn og din Java Card-PIN-kode.

knappen Send Securely (Send sikkert) En softwareknap, som vises på værktøjslinjen i Microsoft Outlook-e-mail-meddelelser. Ved at klikke på knappen kan du signere og/eller kryptere en Microsoft Outlook-e-mail-meddelelse.

knappen Sign and Encrypt (Signer og krypter) En softwareknap, som vises på værktøjslinjen i Microsoft Office-programmer. Ved at klikke på knappen kan du signere, kryptere eller fjerne kryptering i et Microsoft Office-dokument.

konsol Et centralt sted hvorfra du har adgang til og kan administrere funktionerne og indstillingerne i HP ProtectTools Administrative Console.

Kontaktperson, der er tillid til En person, som har accepteret en invitation til at blive kontaktperson, der er tillid til.

Kontaktperson, der er tillid til-invitation En e-mail, som sendes til en person, hvori denne bliver inviteret til at blive kontaktperson, der er tillid til.

Kontaktperson, der er tillid til-modtager En person, som modtager en invitation til at blive kontaktperson, der er tillid til.

kontrolpanel Et centralt sted hvorfra du har adgang til og kan administrere funktionerne og indstillingerne i Security Manager for HP ProtectTools.

kryptering Procedure, f.eks. brugen af en algoritme, der anvendes i kryptografi til at konvertere almindelig tekst til ciffertekst for at forhindre uautoriserede modtagere i at læse disse data. Der findes mange typer datakryptering, og de udgør grundlaget for netværkssikkerhed. Almindelige typer kan være Data Encryption Standard og offentlig nøglekryptering.

kryptografi Praksis med kryptering og dekryptering af data, så de kun kan afkodes af bestemte personer.

legitimationsoplysninger En metode, hvorefter en bruger beviser berettigelse til at bestemt opgave i godkendelsesprocessen.

Liste over kontaktpersoner, der er tillid til En oversigt over kontaktpersoner, der er tillid til.

Live Messenger History Viewer En Privacy Manager Chat-komponent, som gør det muligt at søge efter og få vist krypterede chathistoriksessioner.

logon Et objekt i Security Manager, der består af et brugernavn og en adgangskode (og muligvis andre valgte oplysninger), der kan anvendes til at logge på websteder eller andre programmer.

makulere Udførelsen af en algoritme, som tilslører dataene indeholdt i et aktiv.

makuleringscyklus Det antal gange, som makuleringsalgoritmen udføres på hvert aktiv. Jo højere antal makuleringscyklusser, du vælger, jo mere sikker er computeren.

makuleringsprofil En angivet sletningsmetode og liste over aktiver.

manuel makulering Øjeblikkelig makulering af et aktiv eller udvalgte aktiver, som omgår planen for automatisk makulering.

meddelelse, der er tillid til En kommunikationssession, under hvilken betroede meddelelser sendes fra en betroet afsender til en kontaktperson, der er tillid til.

motiv Et foto af en registreret bruger der anvendes ved godkendelse.

netværkskonto Windows-bruger eller administratorkonto enten på en lokal computer, i en arbejdsgruppe eller på et domæne.

nødgendannelsesarkiv Beskyttet lagerområde, der giver mulighed for genkryptering af basisbrugernøgler fra en platforms ejernøgle til en anden.

overflytning En handling, som muliggør administration, gendannelse og overførsel af Privacy Manager-certifikater og kontaktpersoner, der er tillid til.

PIN Personligt identifikations nummer (PIN-kode).

PKI Public Key Infrastructure-standard, som definerer grænsefladerne for oprettelse, brug og administration af certifikater og kryptografiske nøgler.

politik for enhedsadgangsstyring Listen med enheder, som en bruger har adgang til eller er nægtet adgang til.

Privacy Manager-certifikat Digitalt certifikat, som kræver godkendelse, hver gang du anvender det til kryptografiske operationer, som f.eks. signering og kryptering af e-mail-meddelelser og Microsoft Office-dokumenter.

PSD Personal Secure Drive (personligt, sikkert drev), som indeholder et beskyttet lagerområde til følsomme oplysninger.

rensning af ledig plads Den sikre skrivning af vilkårlige data over slettede aktiver for at forvanske indholdet af det slettede aktiv.

SATA-enhedstilstand Dataoverførselstilstand mellem en computer og masselagerenheder, som f.eks. harddiske og optiske drev.

signaturlinje En pladsholder for den visuelle visning af en digital signatur. Når et dokument signeres, vises underskriverens navn og verificeringsmetode. Datoen for signering og underskriverens titel kan også medtages.

sikkerhedskopiere Brug af sikkerhedskopieringsfunktionen til at gemme en kopi af vigtige programoplysninger på et sted uden for programmet. Derefter kan det anvendes til at gendanne oplysningerne af ældre dato på den samme computer eller på en anden.

sikkerhedslogonmetode Den metode, der anvendes til logon på computeren.

simpel sletning Sletning af Windows-henvisningen til et aktiv. Aktivets indhold forbliver på harddisken, indtil tilslørende data overskriver det vha. af rensning af ledig plads.

Single Sign On (Enkelt sign-on) Funktion, der lagrer godkendelsesoplysninger og giver dig mulighed for at bruge Security Manager til at få adgang til internettet og Windows-programmer, der kræver godkendelse med adgangskode.

tasterækkefølge En kombination af bestemte taster, som, når der trykkes på dem, starter en automatisk makulering, f.eks. ctrl+alt+s.

token Se sikkerhedslogonmetode.

TXT Trusted Execution Technology.

USB-token Sikkerhedsenhed til lagring af identificerende oplysninger om en bruger. Som med et Java Card eller en biometrisk læser anvendes den til at godkende ejeren i forhold til en computer.

Windows-administrator En bruger med fulde rettigheder til at ændre tilladelser og administrere andre brugere.

Windows-brugerkonto Profil for en person, der er autoriseret til at logge på et netværk eller på en enkeltcomputer.

Windows Logon Security Beskytter din/dine Windows-konto(konti) ved at kræve brugen af specifikke legitimationsoplysninger for at få adgang.

virtuelt token Sikkerhedsfunktion, som fungerer meget lig et Java Card og en kortlæser. Dette token gemmes enten på computerens harddisk eller i Windows-registreringsdatabasen. Når du logger på med et virtuelt token, bliver du bedt om en bruger-PIN-kode for at udføre godkendelsen.

vise Handling, som gør det muligt for brugeren at dekryptere én eller flere chathistoriksessioner, så kontaktskærmsnavn(e) vises i almindelig tekst, og sessionen bliver tilgængelig for visning.

Indeks

Å