HP ProtectTools
Brukerhåndbok

Første utgave: November 2009

Dokumentets delenummer: 593308-091

Innhold

1 Presentasjon av sikkerhet

HP ProtectTools Security Manager-programvaren inneholder sikkerhetsfunksjoner som beskytter mot uautorisert tilgang til datamaskinen, nettverk og kritiske data. Administrasjon av HP ProtectTools Security Manager skjer via funksjonen Administrative Console (administrasjonskonsoll).

Ved hjelp av HP ProtectTools Administrative Console (administrasjonskonsoll) kan den lokale administratoren utføre følgende oppgaver:

- Aktivere eller deaktivere sikkerhetsfunksjoner
- Registrere deres fingeravtrykk og fingeravtrykkene til andre brukere av datamaskinen
- Registrere en eller flere scener for ansiktsgjenkjenning
- Konfigurere et smartkort for godkjenning
- Angi nødvendig påloggingsinformasjon for godkjenning
- Administrere brukerne av datamaskinen
- Tilpasse enhetsspesifikke parametere
- Konfigurere installerte Security Manager-programmer
- Legge til flere Security Manager-programmer

Ved hjelp av Security Manager-instrumentbordet kan vanlige brukere utføre følgende oppgaver:

- Konfigurere alternativer som gis av en administrator
- Tillate begrenset styring av enkelte HP ProtectTools-moduler

Programmodulene som er tilgjengelig for datamaskinen, kan variere fra modell til modell.

HP ProtectTools-programmoduler kan være forhåndsinstallert, forhåndslastet eller tilgjengelig for nedlasting fra HPs nettsted. Du finner mer informasjon på nettstedet http://www.hp.com.

MERK: Veiledningen i denne håndboken tar utgangspunkt i at du allerede har installert de aktuelle HP ProtectTools-programmodulene.

HP ProtectTools-funksjoner

Tabellen nedenfor gir en oversikt over hovedfunksjonene i HP ProtectTools-modulene.

Modul	Hovedfunksjoner
HP ProtectTools Security Manager Administrative Console (administrasjonskonsoll, for administratorer)	• Installere og konfigurere nivåer av sikkerhet og sikkerhetspåloggingsmetoder ved hjelp av Security Manager Setup Wizard (installasjonsveiviser). • Konfigurere alternativer som er skjult for vanlige brukere. • Konfigurere konfigurasjoner og brukertilgang for Device Access Manager (tilgangsbehandling). • Legge til og fjerne HP ProtectTools-brukere og vise brukerstatus med administrative verktøy.
HP ProtectTools Security Manager (for vanlige brukere)	• Organisere, konfigurere og endre brukernavn og passord. • Konfigurere og endre brukerlegitimasjon som Windows-passord og smartkort. • Konfigurere og endre File Sanitizer-makulering, bleking og innstillinger. • Vise innstillinger for Device Access Manager (tilgangsbehandling). • Konfigurere innstillinger og alternativer for sikkerhetskopiering og gjenoppretting.
Credential Manager (legitimasjonsbehandling) for HP ProtectTools (Password Manager – passordbehandling)	• Lagre, organisere og beskytte navn og passord. • Konfigurere påloggingsskjermbildene til nettsteder og programmer for rask og sikker tilgang. • Lagre navn og passord til nettsteder ved å registrere dem i Password Manager (passordbehandling). Neste gang du besøker nettstedet, vil Password Manager (passordbehandling) fylle ut og sende opplysningene automatisk. • Lag strengere passord for bedre kontosikkerhet. Password Manager (passordbehandling) fyller ut og sender opplysningene automatisk.
Drive Encryption (stasjonskryptering) for HP ProtectTools (kun på enkelte modeller)	• Sørg for for full harddiskkryptering av hele volumet. • Krev autentisering før oppstart for å dekryptere og gi tilgang til data.
Privacy Manager (personvern) for HP ProtectTools (kun på enkelte modeller)	• Bruk avanserte påloggingsteknikker for å bekrefte kilden, integriteten og sikkerheten ved kommunikasjon via e-post, Microsoft® Office-dokumenter og direktemeldinger (IM).

Modul	Hovedfunksjoner
File Sanitizer (filrensing) for HP ProtectTools	• Makuler digitale aktiva (sensitive opplysninger, inkludert programfiler, historisk eller webrelatert innhold og andre fortrolige data) på datamaskinen og "bleke" harddisken regelmessig.
Device Access Manager (tilgangsbehandling) for HP ProtectTools (kun på enkelte modeller)	• La IT-ledere styre tilgangen til enheter på grunnlag av brukerprofiler. • Hindre at uautoriserte brukere fjerner data ved hjelp av eksterne lagringsmedier og smitter systemet med virus fra eksterne medier. • La administratorer deaktivere tilgangen til skrivbare enheter for bestemte enkeltpersoner eller grupper av brukere.

Oppnå viktige sikkerhetsmål

HP ProtectTools-modulene kan arbeide sammen for å finne løsninger på en rekke sikkerhetsproblemer, inkludert følgende viktige sikkerhetsmål:

- Beskytte mot tyveri
- Begrense tilgang til sensitive data
- Hindre uautorisert tilgang fra interne eller eksterne plasseringer
- Opprette sterke passordpolicyer

Beskyttet mot målrettet tyveri

Et eksempel på et målrettet tyveri vil være tyveri av en datamaskin som inneholder konfidensielle data og kundeinformasjon, i sikkerhetskontrollen på en flyplass. Følgende funksjoner bidrar til å beskytte mot målrettet tyveri:

- Når funksjonen for godkjenning før oppstart er aktivert, hindrer den tilgang til operativsystemet. Se følgende fremgangsmåter:
  - Security Manager (sikkerhetsbehandling)
  - Drive Encryption (stasjonskryptering)

Begrense tilgangen til sensitive data

Tenk deg at en representant for en oppdragsgiver har fått tilgang til en datamaskin i deres lokaler for å gå gjennom sensitive økonomidata. Dere ønsker ikke at kunden skal kunne skrive ut filer eller lagre dem på skrivbare medier som en CD-plate. Følgende funksjon bidrar til å begrense tilgangen til data:

- Med Device Access Manager (tilgangsbehandling) for HP ProtectTools kan IT-ledere begrense tilgangen til skrivbare medier, slik at sensitiv informasjon ikke kan skrives ut eller kopieres fra harddisken til flyttbare medier.

Hindre uautorisert tilgang fra interne eller eksterne steder

Uautorisert tilgang til en usikret bedrifts-PC utgjør en betydelig risiko for bedriftsnettverksressurser som informasjon fra finanstjenester, en leder eller et forsknings- og utviklingsteam, og for personlige opplysninger som pasientjournaler og økonomiske disposisjoner. Disse funksjonene hjelper deg med å hindre uautorisert tilgang:

- Når funksjonen for godkjenning før oppstart er aktivert, hindrer den tilgang til operativsystemet. Se følgende fremgangsmåter:
  - Password Manager (passordbehandling)
  - Drive Encryption (stasjonskryptering)
- Password Manager (passordbehandling) sørger for at uautoriserte brukere ikke kan få passord eller tilgang til passordbeskyttede programmer.
- Med Device Access Manager (tilgangsbehandling) for HP ProtectTools kan IT-ledere begrense tilgangen til skrivbare medier, slik at sensitiv informasjon ikke kan kopieres fra harddisken.

- File Sanitizer (filrensing) muliggjør sikker sletting av data ved å makulere kritiske filer og mapper eller bleke harddisken (overskriving av data som er slettet, men som fremdeles kan gjenopprettes).
- DriveLock bidrar til å sikre at data ikke blir tilgjengelige selv om harddiskstasjonen tas ut og installeres i et usikret system.

Lage sikre passordregler

Hvis det innføres et påbud om bruk av sikre passordregler for flere titalls nettbaserte programmer og databaser, sørger Security Manager (sikkerhetsbehandling) for et beskyttet oppbevaringssted for passord og praktisk engangspålogging (Single Sign On).

Ekstra sikkerhetselementer

Tilordne sikkerhetsroller

Når du administrerer datasikkerheten, er det viktig å dele ansvar og rettigheter blant de forskjellige typene administratorer og brukere (dette gjelder spesielt større organisasjoner).

MERK: I en mindre organisasjon eller ved individuell bruk kan én person inneha alle disse rollene.

Med HP ProtectTools kan du dele sikkerhetspliktene og -rettighetene inn i følgende roller:

- Security officer (sikkerhetsansvarlig) – definerer sikkerhetsnivået for bedriften eller nettverket og bestemmer hvilke sikkerhetsfunksjoner som skal brukes, for eksempel Java™-kort, biometriske lesere eller USB-token.

  MERK: Mange av funksjonene i HP ProtectTools kan tilpasses av den sikkerhetsansvarlige i samarbeid med HP. Hvis du vil ha mer informasjon, se HPs nettsted på http://www.hp.com.

- Administrator – Bruker og styrer sikkerhetsfunksjonene som er angitt av sikkerhetslederen. Kan også aktivere og deaktivere enkelte funksjoner. Hvis sikkerhetslederen har besluttet å innføre Java-kort, kan IT-administratoren for eksempel aktivere BIOS-sikkerhetsmodus for Java-kort.

- Users (brukere) – bruker sikkerhetsfunksjonene. Hvis sikkerhetsansvarlig og IT-administratoren for eksempel har aktivert Java-kort i systemet, kan brukeren angi PIN-koden for Java-kortet og bruke kortet til godkjenning.

FORSIKTIG: Administratorer anbefales å følge "anbefalt praksis" når det gjelder begrensning av brukerrettigheter og brukertilgang.

Uautoriserte brukere bør ikke innvilges administrative rettigheter.

Administrere HP ProtectTools-passord

De fleste funksjonene i HP ProtectTools Security Manager er beskyttet med passord. Tabellen nedenfor viser passordene som ofte brukes, programmodulen der passordet er angitt og passordfunksjonen.

Passordene som angis og bare brukes av IT-administratorer, vises også i tabellen. Alle andre passord kan angis av vanlige brukere eller administratorer.

HP ProtectTools-passord	Angis i følgende modul	Funksjon
Windows-påloggingspassord	Windows® Kontrollpanel eller HP ProtectTools Security Manager	Kan brukes til manuell pålogging og til godkjenning for å få tilgang til ulike Security Manager-funksjoner.
Sikkerhetskopierings- og gjenopprettingspassord i Security Manager (sikkerhetsbehandling)	Security Manager, av enkeltbruker	Beskytter tilgangen til Security Managers sikkerhetskopierings- og gjenopprettingsfil.
PIN-kode for Java™-kort	Java Card Security	Beskytter tilgangen til Java-kortinnholdet og godkjenner Java-kortbrukerne. PIN-koden for Java-kortet beskytter også tilgangen til Computer Setup-programmet og innholdet på datamaskinen når den brukes til godkjenning før oppstart. Godkjenner brukere av Drive Encryption hvis Java-korttokenet er valgt.

Lage et sikkert passord

Når du oppretter passord, må du først følge spesifikasjonene som er angitt i programmet. Generelt sett bør du merke deg følgende for å opprette sterke passord og redusere risikoen for at noen knekker passordet ditt:

- Bruk passord med mer enn 6 tegn, helst med mer enn 8.
- Bland store og små bokstaver i passordet.
- Hvis mulig bør du blande alfanumeriske tegn og inkludere spesialtegn og skilletegn.
- Bytt ut bokstavene i passordet med spesialtegn eller tall. Du kan for eksempel bruke tallet 1 i stedet for bokstavene I eller L.
- Kombiner ord fra to eller flere språk.
- Del opp et ord eller en frase med tall eller spesialtegn, for eksempel "Mary2-2Cat45".
- Ikke bruk et passord som kan slås opp i en ordbok.
- Ikke bruk navnet ditt eller annen personlig informasjon som passord, for eksempel fødselsdato, navn på kjæledyr eller mors pikenavn, heller ikke skrevet baklengs.
- Endre passordet regelmessig. Du kan også endre bare et par tegn hver gang.
- Hvis du skriver ned passordet, må du ikke lagre det på et synlig sted i nærheten av datamaskinen.
- Ikke lagre passordet i en fil på datamaskinen, for eksempel i en e-postmelding.
- Ikke del konto med andre eller gi passordet ditt til noen.

Sikkerhetskopiere og gjenopprette HP ProtectTools-påloggingsinformasjon

Du kan bruke funksjonen Backup and Restore (sikkerhetskopier og gjenopprett) i HP ProtectTools til å velge og sikkerhetskopiere påloggingsinformasjon og innstillinger for HP ProtectTools.

2 Komme i gang med Setup Wizard (installasjonsveiviser)

HP ProtectTools Setup Wizard (installasjonsveiviser) leder deg gjennom konfigureringen av de mest brukte funksjonene i Security Manager. Det finnes imidlertid et vell av tilleggsfunksjoner som er tilgjengelig via HP ProtectTools Administrative Console (administrasjonskonsoll). De samme innstillingene som finnes i veiviseren, i tillegg til andre sikkerhetsfunksjoner, kan konfigureres via konsollen, som du får tilgang til via Start-menyen i Windows®. Disse innstillingene gjelder for datamaskinen og alle brukerne som deler datamaskinen.

1. En uke etter at datamaskinen ble konfigurert vil HP ProtectTools-installasjonsveiviseren starte automatisk for å lede deg gjennom den grunnleggende konfigureringen av programmet når du logger deg på eller en bruker med administrative rettigheter drar en finger over fingeravtrykksleseren for første gang. Et videolæreprogram om konfigurering av datamaskinen starter automatisk.

   – eller –

   Åpne HP ProtectTools Security Manager fra ikonet **Gadget** (miniprograam) i Windows-sidepanelet eller ikonet i systemstatusfeltet lengst til høyre på oppgavelinjen.

   

   Fargen på øverste linje i ikonet Gadget (miniprogram) angir en av disse tilstandene:

   - Rød – HP ProtectTools er ikke konfigurert eller det har oppstått en feiltilstand i en av ProtectTools-modulene.
   - Gul – Sjekk siden Applications Status (programstatus) i Security Manager for eventuelle innstillinger som må endres.
   - Blå – HP ProtectTools er konfigurert og fungerer som det skal.

   MERK: Ikonet Gadget (miniprogram) er ikke tilgjengelig i Windows XP.

   – eller –

Klikk på **Start**, **Alle programmer** og deretter på **HP ProtectTools Administrative Console** (administrasjonskonsoll).

2. Les velkomstskjermbildet og klikk på **Neste**.

MERK: På velkomstskjermbildet kan du deaktivere fortsatt visning av veiviseren ved å velge et av alternativene.

3. Setup Wizard (installasjonsveiviser) ber deg om å legitimere deg.

   Skriv inn Windows-passordet ditt eller skann fingeravtrykk med fingeravtrykksleseren, og klikk på **Neste**.

   Hvis du verken har en fingeravtrykksleser eller smartkort, vil du bli bedt om å oppgi Windows-passordet. Du må bruke dette passordet i fremtiden når godkjenning kreves.

   Hvis du ennå ikke har opprettet et Windows-passord, blir du bedt om å gjøre det. Det kreves et Windows-passord for å beskytte Windows-kontoen mot tilgang fra uautoriserte personer, og for å kunne bruke HP ProtectTools Security Manager-funksjoner.

4. Setup Wizard (installasjonsveiviser) vil lede deg gjennom prosessen med å konfigurere sikkerhetsfunksjoner for alle brukerne av datamaskinen:

   - Windows Logon Security (Windows-påloggingssikkerhet) beskytter Windows-konti ved å kreve bruk av bestemt påloggingsinformasjon for å få tilgang.
   - Drive Encryption (stasjonskryptering) beskytter data ved å kryptere harddisker, slik at data blir uleselige for alle uten riktig godkjenning.
   - Pre-Boot Security (sikkerhet før oppstart) beskytter datamaskinen ved å hindre uautoriserte personer tilgang før oppstart av Windows.

     MERK: Pre-Boot Security (sikkerhet før oppstart) er ikke tilgjengelig hvis datamaskinens BIOS ikke støtter funksjonen.

   Når du skal aktivere en sikkerhetsfunksjon, merker du den aktuelle avkrysningsruten. Jo flere funksjoner du merker, desto mer sikker vil datamaskinen bli.

5. På den siste siden i veiviseren klikker du på **Fullfør**.

   Security Manager-instrumentbordet vises.

MERK: Hvis du ikke fullfører veiviseren, vil den bli startet automatisk to ganger til. Deretter kan du få tilgang til veiviseren fra varslingsboblen som vises i systemstatusfeltet helt til høyre på oppgavelinjen (hvis du ikke har deaktivert denne) inntil installeringen er fullført.

3 HP ProtectTools Security Manager Administrative Console (administrasjonskonsoll)

Administrasjon av HP ProtectTools Security Manager skjer via Administrative Console (administrasjonskonsoll).

MERK: Administrasjon av HP ProtectTools krever administratorrettigheter.

Konsollen har følgende funksjoner:

- Aktivere eller deaktivere sikkerhetsfunksjoner
- Administrere brukerne av datamaskinen
- Tilpasse enhetsspesifikke parametere
- Konfigurere Security Manager-programmer
- Legge til flere Security Manager-programmer

▲ Når du skal bruke HP ProtectTools Security Manager-programmer, starter du HP ProtectTools Security Manager fra Start-menyen eller høyreklikker på Security Manager-ikonet i systemstatusfeltet helt til høyre på oppgavelinjen.

HP ProtectTools Administrative Console (administrasjonskonsoll) og programmene der er tilgjengelig for alle brukere som deler datamaskinen.

Åpne Administrative Console (administrasjonskonsoll)

Når du skal utføre administrative oppgaver, som å angi systemregler eller konfigurere programvare, åpner du konsollen på denne måten:

- Klikk på **Start**, **Alle programmer**, **HP** og deretter på **HP ProtectTools Administrative Console** (administrasjonskonsoll).

  – eller –

  Klikk på **Administration** (administrasjon) til venstre på Security Manager-instrumentbordet.

Når det gjelder brukeroppgaver, som registrering av fingeravtrykk eller bruk av Security Manager, åpner du konsollen på denne måten:

- Klikk på **Start**, **Alle programmer**, **HP** og deretter på **HP ProtectTools Security Manager**.

  – eller –

  Dobbeltklikk på **HP ProtectTools Security Manager**-ikonet i systemstatusfeltet helt til høyre på oppgavelinjen.

Bruke Administrative Console (administrasjonskonsoll)

Security Manager Administrative Console (administrasjonskonsoll) er det sentrale stedet for administrasjon av HP ProtectTools Security Manager.

Konsollen består av følgende komponenter:

- **Tools** (verktøy) – Inneholder disse kategoriene for konfigurering av sikkerhet på datamaskinen:
  - **Home** (hjem) – Her kan du velge sikkerhetsoppgavene som skal utføres.
  - **System** – Her kan du konfigurere sikkerhetsfunksjoner og godkjenning av brukere og enheter.
  - **Applications** (programmer) – Inneholder generelle innstillinger for HP ProtectTools Security Manager og Security Manager-programmer.
  - **Data** – Her finner du en utvidet meny med lenker til Security Manager-programmer som beskytter data.
- **Management Tools** (administrasjonsverktøy) – Inneholder informasjon om flere verktøy. Panelet viser disse valgmulighetene:
  - **HP ProtectTools Security Manager Setup Wizard** (installasjonsveiviser) – Leder deg gjennom konfigureringen av HP ProtectTools Security Manager.
  - **Help** (hjelp) – Viser denne hjelpefilen, som inneholder informasjon om Security Manager og forhåndsinstallerte programmer. Hjelp til programmer som du legger inn, finner du i disse programmene.
  - **About** (om) – Viser informasjon om HP ProtectTools Security Manager, som versjonsnummer og informasjon om opphavsrett.
- **Hovedområde** – Viser programspesifikke skjermbilder.

4 Konfigurere systemet

Du får tilgang til System-gruppen fra menypanelet Tools (verktøy) til venstre i HP ProtectTools Administrative Console-skjermbildet. Du kan bruke programmene i denne gruppen til å administrere reglene og innstillingene for datamaskinen og dens brukere og enheter.

Disse programmene er inkludert i System-gruppen:

- **Security** (sikkerhet) – Administrer funksjoner, godkjenning og innstillinger som bestemmer hvordan brukere samhandler med datamaskinen.
- **Users** (brukere) – Konfigurer, administrer og registrer brukere av datamaskinen.
- **Devices** (enheter) – Administrer innstillinger for sikkerhetsenheter som er innebygd i eller koblet til datamaskinen.

Konfigurere godkjenning for datamaskinen

I programmet Authentication (godkjenning) kan du velge hvilke sikkerhetsfunksjoner som skal implementeres på datamaskinen, angi regler angående tilgang til datamaskinen og konfigurere flere avanserte innstillinger. Du kan angi hva slags påloggingsinformasjon som skal kreves for å godkjenne hver klasse av brukere ved pålogging av Windows eller nettsteder og programmer i løpet av en brukerøkt.

Slik konfigurerer du godkjenning på datamaskinen:

1. Klikk på **Authentication** (godkjenning) på menypanelet Security (sikkerhet).
2. Hvis du skal konfigurere påloggingsgodkjenning, klikker du på kategorien **Logon Policy** (påloggingsregler) og deretter på **Bruk**.
3. Hvis du skal konfigurere øktgodkjenning, klikker du på kategorien **Session Policy** (øktregler) og deretter på **Bruk**.

Påloggingsregler

Slik angir du regler som bestemmer hva slags påloggingsinformasjon som kreves for å godkjenne brukere ved pålogging i Windows:

1. Klikk på **Security** (sikkerhet) på menyen Tools (verktøy), og klikk deretter på **Authentication** (godkjenning).
2. Klikk på en kategori av brukere under **Logon Policy** (påloggingsregler).
3. Angi hva slags påloggingsinformasjon som kreves for å godkjenne den valgte kategorien av brukere. Du må angi minst én type påloggingsinformasjon.
4. Angi om bare én (ANY) av de angitte typene påloggingsinformasjon er påkrevd eller om all (ALL) angitt påloggingsinformasjon er påkrevd for å godkjenne en bruker. Du kan også nekte en bruker tilgang til datamaskinen.
5. Klikk på **Bruk**.

Øktregler

Slik angir du regler som bestemmer hva slags påloggingsinformasjon som kreves for å få tilgang til HP ProtectTools-programmer i en Windows-økt:

1. Klikk på **Security** (sikkerhet) på menyen Tools (verktøy), og klikk deretter på **Authentication** (godkjenning).
2. Klikk på en kategori av brukere under **Session Policy** (øktregler).
3. Angi hva slags påloggingsinformasjon som kreves for å godkjenne den valgte kategorien av brukere.
4. Angi om bare én (ONE) av de angitte typene påloggingsinformasjon er påkrevd eller om all (ALL) angitt påloggingsinformasjon er påkrevd for å godkjenne en bruker. Du kan også angi at det ikke kreves påloggingsinformasjon for å få tilgang til HP ProtectTools-programvare.
5. Klikk på **Bruk**.

Innstillinger

Du kan angi en eller flere av disse sikkerhetsinnstillingene:

- **Allow One Step logon** (tillat engangspålogging) – Tillater brukere av datamaskinen å hoppe over Windows-pålogging hvis godkjenning er foretatt på BIOS- eller kryptert disknivå.
- **Allow HP SpareKey authentication for Windows logon** (tillat HP SpareKey-godkjenning for Windows-pålogging) – Tillater brukere av datamaskinen å bruke HP SpareKey-funksjonen til pålogging i Windows på tross av eventuelle andre godkjenningsregler som er påkrevd i Security Manager (sikkerhetsbehandling).

Slik redigerer du innstillingene:

1. Klikk for å aktivere eller deaktivere en bestemt innstilling.
2. Klikk på **Bruk** for å lagre endringene du har gjort.

Administrere brukere

I programmet Users (brukere) kan du overvåke og administrere datamaskinens HP ProtectTools-brukere.

Alle HP ProtectTools-brukere er oppført og kontrolleres mot reglene som er angitt i Security Manager (sikkerhetsbehandling), og det sjekkes om de har registrert den nødvendige påloggingsinformasjonen for å oppfylle reglene.

Hvis du skal administrere brukere, er følgende innstillinger tilgjengelig:

- Klikk på **Add** (legg til) for å legge til flere brukere.
- Klikk på en bruker og deretter på **Delete** (slett) for å slette en bruker.
- Hvis du skal registrere fingeravtrykk eller konfigurere mer påloggingsinformasjon for en bruker, klikker du på brukeren og deretter på **Enroll** (registrer).
- Hvis du vil se på reglene for en bestemt bruker, velger du brukeren og ser på reglene i det nedre vinduet.

Angi innstillinger for enheter

I programmet Device (enhet) kan du angi innstillinger for innebygde eller tilkoblede sikkerhetsenheter som HP ProtectTools Security Manager har støtte for.

Fingeravtrykk

Siden "Fingerprints" (fingeravtrykk) har tre kategorier: Enrollment (registrering), Sensitivity (følsomhet) og Advanced (avansert).

Registrering

Du kan angi det minste og største antall fingertrykk som en bruker kan registrere.

Du kan også fjerne alle data fra fingeravtrykksleseren.

△ **FORSIKTIG:** Hvis du fjerner alle data fra fingeravtrykksleseren, slettes alle fingeravtrykksdata for alle brukere, også administratorer. Hvis påloggingsreglene kun krever fingeravtrykk, kan alle brukere bli hindret i å logge seg på datamaskinen.

Følsomhet

Flytt på glidebryteren for å stille inn følsomheten for fingeravtrykksleseren når den skanner fingeravtrykk.

Hvis fingeravtrykket ikke avleses konsistent, kan det være nødvendig med en lavere følsomhetsinnstilling. En høyere innstilling øker følsomheten for variasjoner i fingeravtrykklesingen og reduserer dermed risikoen for uriktig godkjenning. En middels-høy innstilling er en god avveining mellom sikkerhet og hva som er praktisk.

Avansert

Du kan konfigurere fingeravtrykksleseren for å spare strøm når datamaskinen går på batteri.

Smartkort

Du konfigurere datamaskinen for å låse seg automatisk når smartkortet tas ut. Datamaskinen vil imidlertid bare låse seg hvis smartkortet ble brukt som påloggingsinformasjon for godkjenning ved pålogging i Windows. Hvis du tar ut et smartkort som ikke ble brukt til å logge på Windows, vil ikke datamaskinen bli låst.

▲ Velg dette alternativet for å aktivere eller deaktivere låsing av datamaskinen når et smartkort tas ut.

Ansikt

Du kan angi sikkerhetsnivået for ansiktsgjenkjenning for å balansere brukervennlighet og hvor vanskelig det skal være å bryte sikkerheten på datamaskinen.

1. Klikk på **Start**, **Alle programmer**, **HP** og deretter på **HP ProtectTools Administrative Console** (administrasjonskonsoll).
2. Klikk på **Devices** (enheter) og deretter på **Face** (ansikt).

3. Hvis du ønsker mer brukervennlighet, flytter du glidebryteren mot venstre. Hvis du ønsker med nøyaktighet, flytter du den mot høyre.

   - **Convenience** (brukervennlighet) – Hvis du vil gjøre det enklere for registrerte brukere å få tilgang i marginale situasjoner, klikker du på glidebryteren for å sette den i stillingen **Convenience** (brukervennlighet).
   - **Balance** (balanse) – Hvis du ønsker et godt kompromiss mellom sikkerhet og brukervennlighet, eller hvis du har sensitiv informasjon eller datamaskinen er plassert i et område hvor uautoriserte påloggingsforsøk kan forekomme, klikker du på glidebryteren for å sette den i stillingen **Balance** (balanse).
   - **Accuracy** (nøyaktighet) – Hvis du vil gjøre det vanskeligere for en bruker å få tilgang når registrerte scener eller lysforholdene ikke er optimale, og mindre sannsynlig at falske godkjenninger inntreffer, klikker du på glidebryteren for å sette den i stillingen **Accuracy** (nøyaktighet).

MERK: Sikkerhetsnivået gjelder for alle brukere

4. Klikk på **Bruk**.

Avanserte innstillinger

1. Klikk på **Start**, **Alle programmer**, **HP** og deretter på **HP ProtectTools Administrative Console** (administrasjonskonsoll).
2. Klikk på **Devices** (enheter) og deretter på **Face** (ansikt).
3. Klikk på **Advanced** (avansert).
   - **Do not require user name for Windows logon (ikke krev brukernavn ved Windows-pålogging).**
     - Merk av for dette alternativet for at brukere skal kunne logge seg på Windows uten brukernavn.
     - Opphev merkingen for å kreve brukernavn ved pålogging.
   - **Enforce the use of PIN for face logon** (krev PIN-kode ved ansiktspålogging) – Merk av for dette alternativet for å kreve at alle brukere angir og bruker PIN-koder ved pålogging.
     - **Minimum length allowed for PIN** (minimumslengde for PIN-kode) – Klikk på pil opp for å øke eller på pil ned for å redusere det minste antall tegn som PIN-koden må bestå av.
     - **Maximum length allowed for PIN** (maksimumslengde for PIN-kode) – Klikk på pil opp for å øke eller på pil ned for å redusere det maksimale antall tegn som PIN-koden kan bestå av.
     - **Maximum retries allowed for PIN** (maksimumslengde for PIN-kode) – Klikk på pil opp for å øke eller på pil ned for å redusere det maksimale antall ganger PIN-koden kan forsøkes.
4. Klikk på **OK**.

5 Konfigurere programmer

Du får tilgang til gruppen Applications (programmer) fra menypanelet Security Applications (sikkerhetsprogrammer) til venstre i HP ProtectTools Administrative Console-skjermbildet. Du kan bruke Settings (innstillinger) til å tilpasse virkemåten til installerte HP ProtectTools Security Manager-programmer.

Slik redigerer du programinnstillinger:

1. Klikk på **Settings** (innstillinger) under **Applications** (programmer) på menyen Tools (verktøy).
2. Klikk for å aktivere eller deaktivere en bestemt innstilling.
3. Klikk på **Bruk** for å lagre endringene du har gjort.

Kategorien General (generelt)

Du finner disse innstillingene i kategorien General (generelt):

- **Do not automatically launch the Setup Wizard for administrators** (ikke start installasjonsveiviseren automatisk for administratorer) – Velg dette alternativet for å unngå at veiviseren starter automatisk ved pålogging.
- **Do not automatically launch the Getting Started wizard for users** (ikke start komme i gang-veiviseren automatisk for brukere) – Velg dette alternativet for å unngå at brukerkonfigurering starter automatisk ved pålogging.

Kategorien Applications (programmer)

Innstillingene som vises her, kan bli endret når nye programmer legges til Security Manager (sikkerhetsbehandling). Minimumsinnstillingene som er standard, er som følger:

- **Applications status** (programstatus) – Gjør det mulig å vise status for alle programmer.
- **Password Manager** (passordbehandling) – Aktiverer Password Manager-programmet for alle brukere av datamaskinen.
- **Privacy Manager** (personvern) – Aktiverer Privacy Manager-programmet for alle brukere av datamaskinen.
- **Enable the Discover more button** (aktiver finn mer-knappen) – Gir brukere av datamaskinen mulighet til å legge til programmer i HP ProtectTools Security Manager ved å klikke på **[+] Discover more** (finn mer).

Klikk på **Restore Defaults** (gjenopprett standarder) for å sette alle programmer tilbake til fabrikkinnstillingene.

6 Styringsverktøy

Flere programmer kan være tilgjengelig for å legge til nye styringsverktøy i Security Manager. Administratoren av datamaskinen kan deaktivere denne funksjonen i programmet Settings (innstillinger).

Klikk på **[+] Management tools** (styringsverktøy) for å legge til flere styringsverktøy.

Oppdateringer og meldinger

Hvis du har Internett-forbindelse, kan du gå til DigitalPersona-nettstedet http://www.digitalpersona.com/ for å se etter nye programmer, eller du kan sette opp en tidsplan for automatisk oppdatering.

1. Hvis du ønsker informasjon om nye programmer og oppdateringer, merker du avkrysningsboksen **Keep me informed about new applications and updates** (hold meg informert om nye programmer og oppdateringer).
2. Velg et antall dager for å sette opp en tidsplan for automatisk oppdatering.
3. Klikk på **Check Now** (kontroller nå) for å se etter oppdateringer.

7 HP ProtectTools Security Manager

Ved hjelp av HP ProtectTools Security Manager kan du styrke sikkerheten til datamaskinen betydelig.

Du kan bruke forhåndsinstallerte Security Manager-programmer i tillegg til ekstra programmer som ligger klar til nedlasting fra Internett:

- Administrere pålogging og passord
- Endre passord for Windows®-operativsystemet på en enkel måte
- Angi programinnstillinger
- Bruke fingeravtrykk som en ekstra sikkerhet og bekvemmelighet
- Registrere en eller flere scener for godkjenning
- Konfigurere smartkort for godkjenning
- Sikkerhetskopiere og gjenopprette programdata
- Legge til flere programmer

Åpne HP ProtectTools Security Manager

Du kan åpne HP ProtectTools Security Manager på en av disse måtene:

- Klikk på **Start**, **Alle programmer**, **HP** og deretter på **HP ProtectTools Security Manager**.
- Dobbeltklikk på **HP ProtectTools**-ikonet i systemstatusfeltet helt til høyre på oppgavelinjen.
- Høyreklikk på **HP ProtectTools**-ikonet og klikk på **Open HP ProtectTools Security Manager** (åpne).
- Klikk på verktøyet **Security Manager ID Card** (ID-kort) i Windows-sidepanelet.
- Bruk direktetastkombinasjonen ctrl+Windows+h for å åpne menyen Security Manager Quick Links (hurtiglenker).

Bruke Security Manager-instrumentbordet

Security Manager-instrumentbordet er det sentrale stedet for enkel tilgang til funksjoner, programmer og innstillinger i Security Manager.

▲ Klikk på **Start**, **Alle programmer**, **HP** og deretter på **HP ProtectTools Security Manager** for å åpne Security Manager-instrumentbordet.

Instrumentbordet består av følgende komponenter:

- **ID Card** (ID-kort) – Viser Windows-brukernavnet og et valgt bilde som identifiserer brukeren som er logget på.
- **Security Applications** (sikkerhetsprogrammer) – Viser en utvidet meny med lenker for konfigurering av følgende sikkerhetskategorier:
  - **Credential Manager (legitimasjonsbehandling)**
  - **My Data (mine data)**
- **Discover more** (finn mer) – Åpner en side hvor du kan finne flere programmer for å forbedre sikkerheten for deg personlig, data og kommunikasjon.
- **Hovedområde** – Viser programspesifikke skjermbilder.
- **Administration** (administrasjon) – Åpner HP ProtectTools Administrative Console (administrasjonskonsoll).
- **Help** (hjelp) – Viser informasjon om det aktuelle skjermbildet.
- **Advanced** (avansert) – Gir tilgang til følgende alternativer:
  - **Preferences** (innstillinger) – Gir deg mulighet til å tilpasse Security Manager-innstillinger.
  - **Backup and Restore** (sikkerhetskopier og gjenopprett) – Gir deg mulighet til å sikkerhetskopiere og gjenopprette data.
  - **About** (om) – Viser versjonsinformasjon om Security Manager.

Installeringsprosedyrer

Registrere påloggingsinformasjon

Du kan bruke siden My Identity (min identitet) til å registrere ulike godkjenningsmetoder eller påloggingsinformasjon. Når disse metodene er registrert, kan du bruke dem til å logge deg på Security Manager.

Registrere fingeravtrykk

Hvis datamaskinen har en fingeravtrykksleser innebygd eller tilkoblet, vil HP ProtectTools Security Manager Setup Wizard (installasjonsveiviser) lede deg gjennom prosessen med å konfigurere eller "registrere" fingeravtrykk.

1. En skisse av to hender vises. Fingrer som allerede er registrert, er fremhevet med grønt. Klikk på en finger på skissen.

   MERK: Hvis du skal slette et registrert fingeravtrykk, klikker du på den aktuelle fingeren.

2. Når du har valgt en finger for registrering, blir du bedt om å skanne fingeren til dette fingeravtrykket er riktig registrert. Registrerte fingrer fremheves med grønt på skissen.

3. Du må registrere minst to fingrer, og peke- og langefingrer foretrekkes. Gjenta trinn 1 til 3 for en annen finger.

4. Klikk på **Neste**, og følg deretter veiledningen på skjermen.

MERK: Når du registrerer fingeravtrykk ved hjelp av Getting Started (komme i gang), blir ikke informasjon om fingeravtrykk lagret før du klikker på **Neste**. Hvis du lar datamaskinen stå urørt en stund eller lukker programmet, blir **ikke** endringene du har gjort lagret.

Registrere scener

Du må registrere en eller flere scener for å bruke ansiktspålogging.

Slik registrerer du en ny scene med HP ProtectTools Security Manager Setup Wizard (installasjonsveiviser):

1. Klikk på ikonet **HP ProtectTools Security Manager** (sikkerhetsbehandling) i sidepanelet på høyre side av skjermen.

2. Skriv inn Windows®-passordet og klikk på **Neste**.

3. Under **Enable security features** (aktiver sikkerhetsfunksjoner) velger du **Windows Logon Security** (Windows-påloggingssikkerhet) og klikker på **Neste**.

4. Under **Choose your credentials** (velg påloggingsinformasjon) velger du **Face** (ansikt) og klikker på **Neste**.

5. Klikk på **Enroll a new scene** (registrer en ny scene).

Når du har registrert deg, kan du også registrere en ny scene hvis du opplever problemer med pålogging fordi ett eller flere av følgende forhold er endret:

- Ansiktet ditt er betydelig endret siden forrige registrering.
- Belysningen er helt forskjellig fra alle dine tidligere registreringer.
- Du brukte briller (eller ikke) ved siste registrering.

MERK: Hvis du har problemer med å registrere scener, kan du forsøke å sette deg nærmere webkameraet. Som ved alle former for fotografering og videofilming, er belysning og kontrast utrolig viktig. Sørg for at belysningen hovedsakelig er i forgrunnen og ikke mest i bakgrunnen. Hvis du opplever at Face Recognition (ansiktsgjenkjenning) ikke godkjenner deg umiddelbart, kan det være verdt å registrere scenen på nytt med bedre belysning.

Slik registrerer du en ny scene med HP ProtectTools Security Manager:

1. Klikk på **Start**, **Alle programmer**, **HP** og deretter på **HP ProtectTools Security Manager** (sikkerhetsbehandling).
2. Klikk på **Credentials** (påloggingsinformasjon) og deretter på **Face** (ansikt).
3. Klikk på **Enroll a new scene** (registrer en ny scene).

Avanserte brukerinnstillinger

1. Klikk på **Start** og **Alle programmer** og deretter på **HP ProtectTools Security Manager**.
2. Klikk på **Set up your authentication credentials** (konfigurer påloggingsinformasjon) og deretter på **Face** (ansikt).
3. Klikk på **Advanced** (avansert) og velg blant disse alternativene.

   a. Hvis bruk av PIN-kode kreves ved ansiktspålogging, klikker du på **Create PIN** (opprett PIN-kode), oppgir Windows-passordet, skriver den nye PIN-koden og bekrefter PIN-koden ved å skrive den på nytt.

   b. Velg flere innstillinger hvis du ønsker det. Disse innstillingene gjelder bare for den aktuelle brukeren:

   - **Play sound on face recognition events (spill av lyd ved ansiktsgjenkjenning)**
     - Merk av for dette alternativet for å spille av en lyd når ansiktsgjenkjenning lykkes eller mislykkes.
     - Opphev merkingen for å deaktivere alternativet.
   - **Prompt to update scenes when logon fails (spør om scener skal oppdateres ved mislykket pålogging)**
     - Merk av for dette alternativet for å la brukeren oppdatere scener hvis påloggingen mislykkes. Hvis kontrollen kommer til "kanskje"-terskelen, blir brukeren bedt om å bestemme om live-bildene i den "mislykkede" påloggingen skal settes inn i gjeldende scene for å øke sjansen for vellykket pålogging neste gang.
     - Opphev merkingen for å deaktivere alternativet.
   - **Prompt to enroll a new scene when logon fails (spør om en ny scene skal registreres ved mislykket pålogging)**
     - Merk av for dette alternativet for å spørre brukeren om å registrere en ny scene hvis ansiktspålogging mislykkes og kontrollen ikke når "kanskje"-terskelen. Dette kan øke sjansen for vellykket pålogging neste gang.
     - Opphev merkingen for å deaktivere alternativet.

   c. Når du skal registrere en ny scene, klikker du på **Enroll a new scene** (registrer en ny scene) og følger veiledningen på skjermen.

Endre Windows-passordet

Security Manager (sikkerhetsbehandling) gjør det enklere og raskere å endre Windows-passord enn via Windows Kontrollpanel.

Følg denne fremgangsmåten for å endre Windows-passordet ditt:

1. Klikk på **Credentials** (påloggingsinformasjon) og deretter på **Password** (passord) fra Security Manager-instrumentbordet.
2. Skriv det gjeldende passordet i tekstboksen **Current Windows password** (gjeldende Windows-passord).

3. Skriv et nytt passord i tekstboksen **New Windows password** (nytt Windows-passord), og skriv det en gang til i tekstboksen **Confirm new password** (bekreft nytt passord).

4. Klikk på **Change** (endre) for å endre det gjeldende passordet til det nye du har oppgitt umiddelbart.

Konfigurere smartkort

Hvis du velger smartkortpålogging og datamaskinen har en smartkortleser innebygd eller tilkoblet, vil Security Manager Setup Wizard (installasjonsveiviser) be deg om å angi en PIN-kode (Personal Identification Number) for smartkortet.

Slik angir du en PIN-kode for smartkort:

1. Oppgi og bekreft en PIN-kode under **Set up smart card** (konfigurer smartkort).

   Du kan også endre PIN-koden. Skriv den gjeldende PIN-koden og deretter den nye.

2. Klikk på **Neste** for å fortsette, og følg deretter veiledningen på skjermen.

– eller –

▲ Klikk på **Credentials** (påloggingsinformasjon) og deretter på **Smart Card** (smartkort) fra Security Manager-instrumentbordet.

- Konfigurere en PIN-kode for smartkort – Oppgi og bekreft en PIN-kode på siden **Set up smart card** (konfigurer smartkort).
- Endre PIN-koden – Skriv først den gjeldende PIN-koden, og oppgi og bekreft deretter den nye.

Generelle oppgaver

Programmene i denne gruppen hjelper deg med å administrere ulike sider ved din digitale identitet.

- **Security Manager** (sikkerhetsbehandling) – Lager og administrerer Quick Links (hurtiglenker), slik at du kan åpne og logge deg på nettsteder og programmer ved hjelp av Windows-passordet, fingeravtrykk eller et smartkort.
- **Credentials** (påloggingsinformasjon) – Gir deg mulighet til å endre Windows-passordet, registrere fingeravtrykk og konfigurere smartkort.

Hvis du vil legge til flere programmer, klikker du på [+] **Discover more** (finn mer) nederst til venstre på instrumentbordet. Denne knappen kan være deaktivert av administratoren.

Password Manager (passordbehandling)

Pålogging av Windows, nettsteder og programmer er enklere og sikrere når du bruker Password Manager (passordbehandling). Du kan bruke dette programmet til å lage gode passord som du ikke må skrive ned eller huske, slik at du kan logge deg på enkelt og raskt med et fingeravtrykk, smartkort eller Windows-passordet.

Password Manager (passordbehandling) gir disse mulighetene:

- Legge til, redigere eller slette påloginger fra kategorien Manage (administrer).
- Bruke hurtiglenker til å åpne standardnettleseren og logge på et nettsted eller program etter at disse er konfigurert.
- Dra og slippe for å ordne hurtiglenkene i kategorier.
- Se med et øyekast om du har passord som utgjør en sikkerhetsrisiko, og automatisk generere et sammensatt, godt passord for nye områder.

Mange funksjoner i Password Manager (passordbehandling) er også tilgjengelig via Password Manager-ikonet som vises når en nettside eller påloggingsskjermbildet til et program har fokus. Klikk på ikonet for å vise en kontekstmeny hvor du kan velge blant alternativene nedenfor.

Nettsider og programmer som det ikke er opprettet pålogging for

Følgende alternativer vises på kontekstmenyen:

- **Add [et_domene.com] to the Password Manager** (legg til et domene) – Gir deg mulighet til å legge inn en pålogging for det aktuelle påloggingsskjermbildet.
- **Open Password Manager** (åpne) – Starter Password Manager.
- **Icon settings** (ikoninnstillinger) – Gir deg mulighet til å angi betingelser for visning av Password Manager-ikonet.
- **Help** (hjelp) – Viser hjelpen til Password Manager (passordbehandling).

Nettsider og programmer som det allerede er opprettet pålogging for

Følgende alternativer vises på kontekstmenyen:

- **Fill in logon data** (fyll ut påloggingsdata) – Legger inn påloggingsdata i påloggingsfeltene og sender siden (hvis sending ble angitt da påloggingen ble definert eller redigert sist).
- **Edit logon** (rediger pålogging) – Gir deg mulighet til å redigere påloggingsdata for nettstedet.
- **Add a New Account** (legg til ny konto) – Gir deg mulighet til å legge en konto til en pålogging.
- **Open Password Manager** (åpne) – Starter Password Manager-programmet.
- **Help** (hjelp) – Viser hjelpen til Password Manager (passordbehandling).

MERK: Administratoren av datamaskinen kan ha konfigurert Security Manager (sikkerhetsbehandling) slik at det kreves mer enn én type påloggingsinformasjon når du skal bekrefte identiteten din.

Legge til påloggінger

Du kan enkelt legge til en pålogging for en nettside eller et program ved å oppgi påloggingsinformasjonen kun én gang. Deretter vil Password Manager (passordbehandling) automatisk oppgi disse opplysningene for deg. Du kan bruke disse påloggingene etter å ha funner frem til nettstedet eller programmet, eller du kan klikke på en pålogging på menyen **Logons** (påloggінger), slik at Password Manager (passordbehandling) åpner nettstedet eller programmet og logger deg på.

Slik legger du inn en pålogging:

1. Åpne påloggingsskjermbildet til nettstedet eller programmet.
2. Klikk på pilen på **Password Manager**-ikonet og deretter på et av følgende, avhengig av om det er påloggingsskjermbildet til et nettsted eller et program:
   - Hvis det er et nettsted, klikker du på **Add [domain name] to Password Manager** (legg til domene).
   - Hvis det er et program, klikker du på **Add this logon screen to Password Manager** (legg til påloggingsskjermbildet).
3. Skriv inn påloggingsinformasjonen. Påloggingsfeltene på skjermen og de tilsvarende feltene i dialogboksen er angitt med tykke oransje rammer. Du kan også vise denne dialogboksen ved å klikke på **Add Logon** (legg til pålogging) fra kategorien **Password Manager Manage** (administrer passordbehandling). Enkelte alternativer er avhengig av hvilke sikkerhetsenheter som er koblet til datamaskinen, for eksempel ved bruk av direktetastene ctrl+Windows+H, skanning av fingeravtrykk eller innsetting av smartkort.
   a. Hvis du vil fylle ut påloggingsfeltene med et av de ferdigformaterte valgene, klikker du på pilene til høyre for feltet.
   b. Hvis du vil vise passordet for påloggingen, klikker du på **Show password** (vis passord).
   c. Hvis du vil fylle ut påloggingsfeltene, men ikke sende dem, opphever du merkingen av **Automatically submit logon data** (send påloggingsdata automatisk).
   d. Klikk på **OK**, klikk på godkjenningsmetoden du vil bruke, **Fingerprints** (fingeravtrykk), **Password** (passord) eller **Face** (ansikt), og logg deg deretter på med den valgte godkjenningsmetoden.

Plusstegnet fjernes fra Password Manager-ikonet for å underrette deg om at påloggingen er opprettet.

e. Hvis Password Manager ikke finner påloggingsfeltene, klikker du på **More fields** (flere felter).

   i. Merk av for hvert felt som kreves ved pålogging, eller opphev merkingen av alle felter som ikke kreves ved pålogging.

   ii. Hvis Password Manager ikke finner alle påloggingsfeltene, vises en melding med spørsmål om du vil fortsette. Klikk på **Ja**.

   iii. Det vises en dialogboks med påloggingsfeltene fylt ut. Klikk på ikonet for hvert felt og dra det til ønsket påloggingsfelt, og klikk deretter på knappen for å logge deg på nettstedet.

   MERK: Når du har brukt den manuelle metoden til å oppgi påloggingsdata for et nettsted, må du fortsette med å bruke denne metoden til å logge deg på det samme nettstedet i fremtiden.

   MERK: Den manuelle måten å oppgi påloggingsdata på er bare tilgjengelig med Internet Explorer 8.

   iv. Klikk på **Lukk**.

Hver gang du går til nettstedet eller åpner programmet, vil Password Manager-ikonet bli vist og angi at du kan bruke den registrerte påloggingsinformasjonen til pålogging.

Redigere påloggінger

Følg denne fremgangsmåten for å redigere en pålogging:

1. Åpne påloggingsskjermbildet til nettstedet eller programmet.
2. Klikk på pilen på **Password Manager**-ikonet og deretter på **Edit logon** (rediger pålogging) for å vise en dialogboks hvor du kan redigere påloggingsdata. Påloggingsfeltene på skjermen og de tilsvarende feltene i dialogboksen er angitt med skarpe oransje rammer.

   Du kan også vise denne dialogboksen ved å klikke på **Edit for the desired logon** (rediger ønsket pålogging) fra kategorien **Password Manager Manage** (administrer).
3. Rediger påloggingsdataene.
   - Hvis du vil fylle ut påloggingsfeltene med et av de ferdigformaterte valgene, klikker du på pilene til høyre for feltet.
   - Hvis du vil legge flere felter fra skjermbildet til påloggingen, klikker du på **More fields** (flere felter).
   - Hvis du vil fylle ut påloggingsfeltene, men ikke sende dem, opphever du merkingen av **Submit logon data** (send påloggingsdata).
   - Hvis du vil vise passordet for påloggingen, klikker du på **Show password** (vis passord).
4. Klikk på **OK**.

Bruke menyen Logons (pålogging)

Password Manager (passordbehandling) har en rask, enkel måte du kan bruke til å starte nettsteder og programmer som du har opprettet påloggінger for. Dobbeltklikk på en program- eller nettstedspålogging

på menyen **Logons** (påloggінger) eller i kategorien **Manage** (administrer) i **Password Manager** for å åpne påloggingsskjermbildet og fylle ut påloggingsdataene.

Når du oppretter en pålogging, legges den automatisk til på menyen Logons (påloggінger) i Password Manager (passordbehandling).

Slik viser du menyen Logons (påloggінger):

1. Bruk direktetastkombinasjonen for **Password Manager** (passordbehandling). Fabrikkinnstillingen er ctrl+Windows+h. Hvis du vil endre direktetastkombinasjonen, klikker du på **Password Manager** (passordbehandling) og deretter på **Settings** (innstillinger).
2. Skann fingeravtrykket ditt (på datamaskiner med innebygd eller tilkoblet fingeravtrykksleser).

Ordne påloggінger i kategorier

Bruk en eller flere kategorier for å holde orden på påloggingene. Du kan dra og slippe påloggingene til ønsket kategori.

Slik legger du til en kategori:

1. Klikk på **Password Manager** (passordbehandling) fra Security Manager-instrumentbordet.
2. Klikk på kategorien **Manage** (administrer) og deretter på **Add Category** (legg til kategori).
3. Gi kategorien et navn.
4. Klikk på **OK**.

Slik ordner du påloggінger i kategorier:

1. Plasser musepekeren over ønsket pålogging.
2. Trykk på og hold venstre museknapp.
3. Dra påloggingen til listen over kategorier. Kategoriene fremheves etter hvert som du flytter musepekeren over dem.
4. Slipp museknappen når ønsket kategori er fremhevet.

Påloggingene blir ikke flyttet til kategoriene, men bare kopiert til den valgte kategorien. Du kan legge samme pålogging i mer enn en kategori, og du kan vise alle påloggingene ved å klikke på **All** (alle).

Administrere påloggінger

Password Manager (passordbehandling) gjør det enkelt å administrere påloggingsdata som brukernavn, passord og flere påloggingskonti på ett sentralt sted.

Du finner påloggingene dine i kategorien Manage (administrer). Hvis det er opprettet flere påloggінger for samme nettsted, er hver pålogging oppført under navnet på nettstedet og innrykket i påloggingslisten.

Slik administrerer du påloggінger:

Klikk på **Password Manager** (passordbehandling) og deretter på **Manage** (administrer) fra Security Manager-instrumentbordet.

- **Legge til pålogging** – Klikk på **Add Logon** (legg til pålogging) og følg veiledningen på skjermen.
- **Redigere pålogging** – Klikk på en pålogging og på **Edit** (rediger), og endre deretter påloggingsdataene.
- **Slette pålogging** – Klikk på en pålogging og på **Delete** (slett).

Slik legger du til flere påloggінger for et nettsted eller program:

1. Åpne påloggingsskjermbildet til nettstedet eller programmet.
2. Klikk på **Password Manager**-ikonet for å vise hurtigmenyen.
3. Klikk på **Add additional logon** (legg til flere påloggінger) og følg veiledningen på skjermen.

Vurdere passordkvaliteten

Bruk av gode passord til pålogging av nettsteder og programmer er en viktig side ved det å beskytte sin identitet.

Password Manager (passordbehandling) gjør det enkelt å overvåke og forbedre sikkerheten med umiddelbar og automatisk analyse av kvaliteten til passordene som brukes til pålogging av nettsteder og programmer.

Innstillinger for Password Manager-ikonet

Password Manager (passordbehandling) forsøker å identifisere påloggingsskjermbildene til nettsteder og programmer. Når Password Manager oppdager et påloggingsskjermbilde du ikke har opprettet noen pålogging for, vil programmet be deg om å legge til en pålogging for skjermbildet ved å vise Password Manager-ikonet med et "+"-tegn.

Klikk på ikonpilen og deretter på **Icon Settings** (ikoninnstillinger) for å tilpasse måten **Password Manager** håndterer mulige påloggingssteder på.

- **Prompt to add logons for logon screens** (be om å legge til påloggінger) – Klikk på dette alternativet for å få Password Manager til å be deg om å legge til en pålogging ved visning av et påloggingsskjermbilde som det ikke er konfigurert noen pålogging for.
- **Exclude this screen** (utelukk dette skjermbildet) – Velg dette alternativet for at Password Manager (passordbehandling) ikke skal be deg om å legge til en pålogging for dette påloggingsskjermbildet på nytt.

Klikk på **Password Manager** og deretter på **Settings** (innstillinger) på Security Manager-instrumentbordet for å få tilgang til flere Password Manager-innstillinger.

Innstillinger

Du kan angi innstillinger for å tilpasse HP ProtectTools Security Manager:

1. **Prompt to add logons for logon screens** (be om å legge til påloginger) – Password Manager-ikonet vises med et plusstegn når påloggingsskjermbildet til et nettsted eller program blir oppdaget, slik at du kan legge til en pålogging for skjermbildet i passordhvelvet. Klikk på **Icon Settings** (ikoninnstillinger) og opphev merkingen av **Prompt to add logons for logon screens** (be om å legge til påloginger) for å deaktivere funksjonen.

2. **Open Password Manager with ctrl+Windows+h** (åpne passordbehandling med ctrl+Windows-h) – Direktetastkombinasjonen som åpner menyen Quick Links (hurtiglenker) i Password Manager (passordbehandling), er ctrl+Windows+h som standard. Du endrer direktetasten ved å klikke på dette alternativet og oppgi en ny tastkombinasjon. Kombinasjonene kan inkludere en eller flere av disse tastene: ctrl, alt, skift og alle bokstav- og talltaster.

3. Klikk på **Bruk** for å lagre endringene.

Påloggingsinformasjon

Du bruker Security Manager-påloggingsinformasjon til å bekrefte identiteten din. Den lokale administratoren av datamaskinen kan angi hva slags påloggingsinformasjon du kan bruke til å bekrefte identiteten din når du logger deg på Windows, nettsteder og programmer.

Hvilken påloggingsinformasjon som er tilgjengelig, kan variere med hvilke sikkerhetsenheter som er innebygd i eller tilkoblet datamaskinen. All påloggingsinformasjon som støttes vil ha en oppføring i gruppen **My Identity, Credentials** (min identitet, påloggingsinformasjon).

Tilgjengelig påloggingsinformasjon, krav og nåværende status er oppført og kan omfatte:

- Fingeravtrykk
- Passord
- Smartkort
- Ansikt

Klikk på lenken og følg veiledningen på skjermen for å registrere eller endre påloggingsinformasjon.

Ditt personlige ID-kort

Ditt ID-kort identifiserer deg entydig som eier av denne Windows-kontoen, og viser navnet ditt og et bilde du velger. Det vises på en fremtredende plass øverst til venstre på Security Manager-sider og som verktøy på Windows-sidepanelet.

Det å klikke på ID-kortet i Windows-sidepanelet er en av mange måter å få rask tilgang til Security Manager (sikkerhetsbehandling) på.

Du kan endre bildet og måten navnet vises på. Som standard vises ditt fulle Windows-brukernavn og bildet du valgte under oppsett av Windows.

Slik endrer du navnet som vises:

1. Klikk på ikonet **ID Card** (ID-kort) øverst til venstre på Security Manager-instrumentbordet.
2. Klikk på avkrysningsboksen med navnet du oppga for Windows-kontoen din. Systemet vil vise Windows-brukernavnet til denne kontoen.
3. Hvis du vil endre navnet, skriver du det nye navnet og klikker på **Save** (lagre).

Slik endrer du bildet som vises:

1. Klikk på **ID Card** (ID-kort) øverst til venstre på Security Manager-instrumentbordet.
2. Klikk på **Choose picture** (velg bilde), på bildet du ønsker og deretter på **Save** (lagre).

Velge innstillinger

Du kan tilpasse innstillingene for HP ProtectTools Security Manager: Klikk på **Advanced** (avansert) og deretter på **Preferences** (innstillinger) fra Security Manager-instrumentbordet. De tilgjengelige innstillingene er delt i to kategorier: General (generelt) og Fingerprint (fingeravtrykk).

Generelt

Du finner disse innstillingene i kategorien General (generelt):

Appearance (utseende) – **Show icon on taskbar** (vis ikon på oppgavelinje)

- Merk av dette alternativet for å vise ikonet på oppgavelinjen.
- Opphev merkingen av dette alternativet for ikke å vise ikonet på oppgavelinjen.

Fingeravtrykk

Du finner disse innstillingene i kategorien Fingerprint (fingeravtrykk):

- **Quick Actions** (hurtighandlinger) – Bruk Quick Actions (hurtighandlinger) til å velge hvilken Security Manager-oppgave som skal utføres når du holder nede en angitt tast mens du skanner fingeravtrykket.

  Hvis du vil tilordne en hurtighandling til en av de oppførte tastene, klikker du på et **(Key) + Fingerprint**-alternativ (tast + fingeravtrykk), og velger deretter en av de tilgjengelige oppgavene fra menyen.

- **Fingerprint Scan Feedback** (tilbakemelding fra fingeravtrykksleser) – Vises bare hvis du har en fingeravtrykksleser. Bruk denne innstillingen for å tilpasse tilbakemeldingen du får når du skanner fingeravtrykk.

  - **Enable sound feedback** (aktiver lydsignal) – Security Manager varsler med et lydsignal når et fingeravtrykk er skannet, og spiller av forskjellige lyder for bestemte programhendelser. Du kan tilordne nye lyder til disse hendelsene via Lyd-kategorien i Windows Kontrollpanel, eller du kan deaktivere lydsignalene ved å oppheve dette valget.

  - **Show scan quality feedback (vis tilbakemelding om skannekvalitet)**

    Merk av for dette alternativet for å vise alle skanninger, uansett kvalitet.

    Opphev merkingen av alternativet for å vise bare skanninger av god kvalitet.

Sikkerhetskopiere og gjenopprette data

Det anbefales at du sikkerhetskopierer Security Manager-data regelmessig. Hvor ofte du bør sikkerhetskopiere, er avhengig av hvor ofte dataene endres. Hvis du for eksempel legger til nye påloginger daglig, bør du sannsynligvis sikkerhetskopiere data daglig.

Sikkerhetskopier kan også brukes til å migrere fra en datamaskin til en annen, noe som også kalles eksport og import.

MERK: Bare data sikkerhetskopieres med denne funksjonen.

HP ProtectTools Security Manager må være installert på alle datamaskiner som skal motta sikkerhetskopierte data, før dataene kan gjenopprettes fra sikkerhetskopifilen.

Slik sikkerhetskopierer du data:

1. Klikk på **Advanced** (avansert) i panelet til venstre og deretter på **Backup and Restore** (sikkerhetskopier og gjenopprett).
2. Klikk på **Back up data** (sikkerhetskopier data).
3. Velg modulene du vil ta med i sikkerhetskopieringen. I de fleste tilfeller vil du velge å ta med alle.
4. Gi lagringsfilen et navn. Som standard vil filen bli lagret i Dokumenter-mappen. Klikk på **Bla gjennom** for å angi en annen plassering.
5. Oppgi et passord for å beskytte filen.
6. Bekreft identiteten din.
7. Klikk på **Fullfør**.

Slik gjenoppretter du data:

1. Klikk på **Advanced** (avansert) i panelet til venstre og deretter på **Backup and Restore** (sikkerhetskopier og gjenopprett).
2. Klikk på **Restore data** (gjenopprett data).
3. Velg lagringsfilen som er opprettet tidligere. Du kan oppgi banen i feltet for dette, eller du kan klikke på **Bla gjennom**.
4. Oppgi passordet som ble brukt til å beskytte filen.
5. Velg modulene med data som du vil gjenopprette. I de fleste tilfeller vil det være alle de oppførte modulene.
6. Klikk på **Fullfør**.

Finn ut mer

Det kan finnes flere programmer med nye funksjoner for dette programmet.

Klikk på **[+] Discover more** (finn ut mer) på Security Manager-instrumentbordet for å se gjennom andre programmer.

MERK: Hvis det ikke er noen **[+] Discover more**-lenke nederst til venstre på instrumentbordet, er den deaktivert av datamaskinens administrator.

Oppdateringer og meldinger

1. Hvis du ønsker informasjon om nye programmer og oppdateringer, merker du avkrysningsboksen **Keep me informed about new applications and updates** (hold meg informert om nye programmer og oppdateringer).
2. Velg et antall dager for å sette opp en tidsplan for automatisk oppdatering.
3. Klikk på **Check Now** (kontroller nå) for å se etter oppdateringer.

Status for sikkerhetsprogrammer

Siden Applications Status (programstatus) i Security Manager (sikkerhetsbehandling) viser samlet status for alle installerte sikkerhetsprogrammer. Siden viser programmer som er konfigurert og konfigurasjonsstatus for hvert av dem. Sammendraget vises automatisk når du åpner Security Manager-instrumentbordet og klikker på **Check the status of the security applications** (sjekk status for sikkerhetsprogrammer), når du klikker på **Security Applications** (sikkerhetsprogrammer) eller når du klikker på **Check Now** (sjekk nå) på ikonet **Gadget** (miniprogram) i Windows-sidepanelet til høyre på skjermen.

8 Drive Encryption (stasjonskryptering) for HP ProtectTools (kun på enkelte modeller)

△ **FORSIKTIG:** Hvis du bestemmer deg for å avinstallere modulen Drive Encryption (stasjonskryptering), må du først dekryptere alle krypterte stasjoner. Hvis du ikke gjør det, kan du ikke få tilgang til dataene på krypterte stasjoner med mindre du har registrert deg hos gjenopprettingstjenesten for Drive Encryption (stasjonskryptering). Installering av modulen Drive Encryption (stasjonskryptering) på nytt vil ikke gi tilgang til de krypterte stasjonene.

Drive Encryption (stasjonskryptering) for HP ProtectTools sørger for full databeskyttelse ved å kryptere datamaskinens harddisk. Når Drive Encryption (stasjonskryptering) er aktivert, må du logge deg på Drive Encryption-påloggingsbildet, som vises før Windows®-operativsystemet starter.

HP ProtectTools Setup Wizard (installasjonsveiviser) gir Windows-administratorer mulighet til å aktivere Drive Encryption (stasjonskryptering), sikkerhetskopiere krypteringsnøkkelen, legge til og fjerne brukere og deaktivere Drive Encryption. Du finner mer informasjon i hjelpen til HP ProtectTools Security Manager-programvaren.

Følgende oppgaver kan utføres med Drive Encryption (stasjonskryptering):

- Krypteringsadministrasjon

  Kryptering eller dekryptering av enkeltstasjoner

  MERK: Bare interne harddisker kan krypteres.

- Gjenoppretting
  - Opprette sikkerhetskopinøkler
  - Foreta en gjenoppretting

Konfigureringsprosedyrer

Åpne Drive Encryption (stasjonskryptering)

1. Klikk på **Start**, **Alle programmer**, **HP** og deretter på **HP ProtectTools Administrative Console** (administrasjonskonsoll).
2. Klikk på **Drive Encryption** (stasjonskryptering) i panelet til venstre.

Generelle oppgaver

Aktivere Drive Encryption (stasjonskryptering)

Bruk HP ProtectTools Setup Wizard (installasjonsveiviser) til å aktivere Drive Encryption (stasjonskryptering).

MERK: Denne veiviseren brukes også til å legge til og fjerne brukere.

– eller –

1. Klikk på **Start**, **Alle programmer**, **HP** og deretter på **HP ProtectTools Administrative Console** (administrasjonskonsoll).
2. Klikk på **Security** (sikkerhet) og deretter på **Features** (funksjoner) i panelet til venstre.
3. Velg **Drive Encryption** (stasjonskryptering) og klikk på **Neste**.
4. Under **Drives to be encrypted** (stasjoner som skal krypteres), merker du harddisken som du vil kryptere.
5. Sett inn lagringsenheten i riktig spor.

   MERK: Hvis du skal lagre krypteringsnøkkelen, må du bruke en USB-lagringsenhet med formatet FAT32.

6. Under **External storage device on which to save encryption key** (ekstern lagringsenhet for lagring av krypteringsnøkkel) velger du lagringsenheten hvor du vil lagre krypteringsnøkkelen.
7. Klikk på **Bruk**.

   Stasjonskrypteringen starter.

Du finner mer informasjon i hjelpen til HP ProtectTools Security Manager-programvaren.

Deaktivere Drive Encryption (stasjonskryptering)

Bruk HP ProtectTools Setup Wizard (installasjonsveiviser) til å deaktivere Drive Encryption (stasjonskryptering). Du finner mer informasjon i hjelpen til HP ProtectTools Security Manager-programvaren.

– eller –

1. Klikk på **Start**, **Alle programmer**, **HP** og deretter på **HP ProtectTools Administrative Console** (administrasjonskonsoll).
2. Klikk på **Security** (sikkerhet) og deretter på **Features** (funksjoner) i panelet til venstre.
3. Opphev merkingen av **Drive Encryption** (stasjonskryptering) og klikk på **Bruk**.

   Dekrypteringen av stasjonen starter.

Logge på med Drive Encryption (stasjonskryptering) aktivert

Når du slår på datamaskinen etter at Drive Encryption (stasjonskryptering) er aktivert og brukerkontoen din er registrert, må du logge deg på i påloggingsskjermbildet til Drive Encryption (stasjonskryptering):

MERK: Hvis Windows-administratoren har aktivert sikkerhet før oppstart i HP ProtectTools Security Manager, logges du på datamaskinen umiddelbart etter at datamaskinen slås på, i stedet for via påloggingsskjermbildet til Drive Encryption (stasjonskryptering).

1. Klikk på brukernavnet ditt og skriv inn Windows-passordet eller PIN-koden til Java™-kortet, eller skann en registrert finger.
2. Klikk på **OK**.

MERK: Hvis du bruker en gjenopprettingsnøkkel til å logge på i påloggingsskjermbildet til Drive Encryption (stasjonskryptering), blir du også bedt om å velge Windows-brukernavnet og skrive inn passordet ditt på påloggingsskjermbildet til Windows.

Beskytte data ved å kryptere harddisken

Bruk HP ProtectTools Setup Wizard (installasjonsveiviser) til å beskytte data ved å kryptere harddisken:

1. Klikk på **Getting Started** (komme i gang) i Security Manager og deretter på ikonet **Security Manager Setup Wizard** (installasjonsveiviser). En demonstrasjon som beskriver Security Manager-funksjoner, starter. (Du kan også starte Security Manager fra siden Drive Encryption (stasjonskryptering).)
2. Klikk på **Drive Encryption** (stasjonskryptering) i panelet til venstre og deretter på **Encryption Management** (krypteringsadministrasjon).
3. Klikk på **Change Encryption** (endre kryptering).
4. Velg stasjonen eller stasjonene som skal krypteres.

MERK: Vi anbefaler sterkt at du krypterer harddisken.

Vise krypteringsstatus

Brukere kan vise krypteringsstatusen i HP ProtectTools Security Manager.

MERK: Endringer i stasjoners krypteringsstatus må gjøres ved hjelp av HP ProtectTools Administrative Console (administrasjonskonsoll).

1. Åpne **HP ProtectTools Security Manager**.
2. Under **My Data** (mine data) klikker du på **Encryption Status** (krypteringsstatus).

   Hvis Drive Encryption (stasjonskryptering) er aktivert, vises en av disse statuskodene:

   - Active (aktiv)
   - Inactive (inaktiv)
   - Not encrypted (ikke kryptert)
   - Encrypted (kryptert)
   - Encrypting (krypteres)
   - Decrypting (dekrypteres)

   Hvis harddisken er i ferd med å bli kryptert eller dekryptert, vil en fremdriftslinje vise hvor mange prosent som er fullført og hvor lang tid det vil ta å fullføre krypteringen eller dekrypteringen.

Avanserte oppgaver

Administrere Drive Encryption (stasjonskryptering, administratoroppgave)

På siden Encryption Management (krypteringsadministrasjon) kan administratorer vise og endre stasjonskrypteringsstatus (aktiv eller inaktiv) og vise krypteringsstatus for alle harddiskstasjoner på datamaskinen.

- Hvis statusen er Inactive (inaktiv), er ikke Drive Encryption (stasjonskryptering) aktivert av Windows-administratoren i HP ProtectTools Security Manager og harddisken beskyttes ikke. Bruk Setup Wizard (installasjonsveiviser) i HP ProtectTools Security Manager til å aktivere stasjonskryptering.
- Hvis statusen er Active (aktiv), er Drive Encryption (stasjonskryptering) aktivert og konfigurert. Stasjonen er da i en av disse tilstandene:
  - Not encrypted (ikke kryptert)
  - Encrypted (kryptert)
  - Encrypting (krypteres)
  - Decrypting (dekrypteres)

Kryptere eller dekryptere enkeltstasjoner

Hvis du skal kryptere en eller flere harddisker på datamaskinen eller dekryptere en kryptert stasjon, bruker du funksjonen Change Encryption (endre kryptering):

1. Åpne **HP ProtectTools Administrative Console** (administrasjonskonsoll) og klikk på **Drive Encryption** (stasjonskryptering) og deretter på **Encryption Management** (krypteringsadministrasjon).
2. Klikk på **Change Encryption** (endre kryptering).
3. I dialogboksen Change Encryption (endre kryptering) velger du eller opphever merkingen av hver harddiskstasjon du vil kryptere eller dekryptere, og deretter klikker du på **OK**.

MERK: Mens stasjonen krypteres eller dekrypteres, viser en fremdriftslinje hvor mye tid som gjenstår før prosessen er fullført i den aktuelle økten. Hvis datamaskinen slås av eller går i hvile-, vente- eller dvalemodus i løpet av krypteringsprosessen og deretter startes på nytt, nullstilles visningen av gjenstående tid, men krypteringen fortsetter der den faktisk stoppet sist. Visningen av gjenstående tid og fremdrift endres deretter raskere for å gjenspeile den tidligere fremdriften.

Sikkerhetskopiering og gjenoppretting (administratoroppgave)

På siden Recovery (gjenoppretting) kan administratorer sikkerhetskopiere og gjenopprette krypteringsnøkler.

Local Drive Encryption Key Backup (sikkerhetskopi av krypteringsnøkkel) – Gir deg mulighet til å sikkerhetskopiere krypteringsnøkler på flyttbare medier hvis Drive Encryption (stasjonskryptering) er aktivert.

Opprette sikkerhetskopinøkler

Du kan sikkerhetskopiere krypteringsnøkkelen til en kryptert stasjon på en flyttbar lagringsenhet:

△ **FORSIKTIG:** Oppbevar lagringsenheten som innholder sikkerhetskopinøkkelen, på et trygt sted. Hvis du glemmer passordet eller mister Java-kortet, er det bare denne enheten som gir tilgang til harddisken.

1. Åpne **HP ProtectTools Administrative Console** (administrasjonskonsoll) og klikk på **Drive Encryption** (stasjonskryptering) og deretter på **Recovery** (gjenoppretting).
2. Klikk på **Backup Keys** (sikkerhetskopinøkler).
3. På siden Select Backup Disk (velg sikkerhetskopidisk) klikker du på navnet på enheten som du vil sikkerhetskopiere krypteringsnøkkelen til, og deretter på **Neste**.
4. Les informasjonen på den neste siden som vises, og klikk deretter på **Neste**. Krypteringsnøkkelen blir lagret på lagringsenheten du valgte.
5. Når bekreftelsesdialogboksen åpnes, klikker du på **Fullfør**.

Foreta en gjenoppretting

Følg denne fremgangsmåten for å utføre en gjenoppretting hvis du glemmer passordet:

1. Slå på datamaskinen.
2. Sett inn den flyttbare lagringsenheten som inneholder sikkerhetskopinøkkelen.
3. Når påloggingsdialogboksen til Drive Encryption (stasjonskryptering) for HP ProtectTools åpnes, klikker du på **Avbryt**.
4. Klikk på **Options** (alternativer) nederst til venstre på skjermbildet og deretter på **Recovery** (gjenoppretting).
5. Velg filen som inneholder sikkerhetskopinøkkelen, eller klikk på **Bla gjennom** for å søke etter den, og klikk deretter på **Neste**.
6. Når bekreftelsesdialogboksen åpnes, klikker du på **OK**.

   Datamaskinen starter.

MERK: Det anbefales på det sterkeste at du tilbakestiller passordet etter å ha utført en gjenoppretting.

9 Privacy Manager (personvern) for HP ProtectTools (kun på enkelte modeller)

Med Privacy Manager (personvern) for HP ProtectTools kan du bruke avanserte sikkerhetspåloggingsmetoder (godkjenning) til å bekrefte kilden, integriteten og sikkerheten for kommunikasjon ved bruk av e-post, Microsoft® Office-dokumenter og direktemeldinger (IM).

Privacy Manager (personvern) håndterer sikkerhetsinfrastrukturen levert av HP ProtectTools Security Manager, og inkluderer følgende sikkerhetspåloggingsmetoder:

- Fingeravtrykkgodkjenning
- Windows®-passord
- HP ProtectTools Java™-kort

Du kan bruke alle sikkerhetspåloggingsmetodene ovenfor i Privacy Manager (personvern).

Privacy Manager krever følgende:

- HP ProtectTools Security Manager 5.00 eller høyere
- Operativsystemet Windows® 7, Windows Vista® eller Windows XP
- Microsoft Outlook 2007 eller Microsoft Outlook 2003
- En gyldig e-postkonto

MERK: Et Privacy Manager-sertifikat (et digitalt sertifikat) må bestilles og installeres i Privacy Manager (personvern) før du får tilgang til sikkerhetsfunksjonene. Se Bestille og installere et Privacy Manager-sertifikat på side 47 for å få informasjon om bestilling av et Privacy Manager-sertifikat.

Konfigureringsprosedyrer

Åpne Privacy Manager (personvern)

Slik åpner du Privacy Manager (personvern):

1. Klikk på **Start**, **Alle programmer**, **HP** og deretter på **HP ProtectTools Security Manager**.
2. Klikk på **Privacy Manager** (personvern).

– eller –

Høyreklikk på **HP ProtectTools**-ikonet i systemstatusfeltet helt til høyre på oppgavelinjen, klikk på **Privacy Manager** (personvern) og deretter på **Configuration** (konfigurasjon).

– eller –

Klikk på nedpilen ved siden av **Send Securely** (send sikkert) på verktøylinjen i en Microsoft Outlook-melding, og klikk deretter på **Certificates** (sertifikater) eller **Trusted Contacts** (klarerte kontakter).

– eller –

Klikk på nedpilen ved siden av **Sign and Encrypt** (signer og krypter) på verktøylinjen i et Microsoft Office-dokument, og klikk deretter på **Certificates** (sertifikater) eller **Trusted Contacts** (klarerte kontakter).

Administrere Privacy Manager-sertifikater

Privacy Manager-sertifikater (personvern) beskytter data og meldinger med en kryptografiteknologi som kalles PKI (Public Key Infrastructure – fellesnøkkelinfrastruktur). PKI krever at brukerne skaffer seg kryptografiske nøkler og et Privacy Manager-sertifikat som er utstedt av en sertifiseringsmyndighet (CA). Til forskjell fra det meste av datakrypterings- og godkjenningsprogramvare, som bare krever periodisk godkjenning, krever Privacy Manager (personvern) godkjenning hver gang du signerer en e-postmelding eller et Microsoft Office-dokument med en kryptografisk nøkkel. Med Privacy Manager (personvern) blir prosessen med lagring og sending av viktig informasjon trygg og sikker.

Du kan utføre disse oppgavene:

- Bestille og installere et Privacy Manager-sertifikat
- Vise detaljer om Privacy Manager-sertifikater
- Fornye Privacy Manager-sertifikater
- Angi et standardsertifikat for Privacy Manager (personvern) hvis flere sertifikater er tilgjengelig
- Slette og tilbakekalle et Privacy Manager-sertifikat (avansert)

Bestille og installere et Privacy Manager-sertifikat

Før du kan bruke funksjonene i Privacy Manager (personvern), må du bestille og installere et Privacy Manager-sertifikat (fra Privacy Manager) ved hjelp av en gyldig e-postadresse. E-postadressen må være konfigurert som en konto i Microsoft Outlook på samme datamaskin som du bestiller Privacy Manager-sertifikat fra.

Bestille et Privacy Manager-sertifikat

1. Åpne Privacy Manager (personvern) og klikk på **Certificates** (sertifikater).
2. Klikk på **Request a Privacy Manager Certificate** (bestille et sertifikat).
3. Les teksten på velkomstsiden og klikk deretter på **Neste**.
4. Les lisensavtalen på siden License Agreement (lisensavtale).
5. Kryss av for **Check here to accept the terms of this license agreement** (merk av her for å godta vilkårene i lisensavtalen), og klikk deretter på **Neste**.
6. Skriv inn nødvendig informasjon på siden Your Certificate Details (dine sertifikatdetaljer) og klikk på **Neste**.
7. Klikk på **Fullfør** på siden "Certificate Request Accepted" (sertifikatbestilling mottatt).
8. Klikk på **OK** for å lukke sertifikatet.

Du vil motta en e-postmelding i Microsoft Outlook med Privacy Manager-sertifikatet vedlagt.

Skaffe et forhåndstildelt Privacy Manager-sertifikat

1. Åpne den mottatte e-postmeldingen om at du har fått et forhåndstildelt firmasertifikat, i Outlook.
2. Klikk på **Obtain** (hent).
3. Du vil motta en e-postmelding i Microsoft Outlook med Privacy Manager-sertifikatet vedlagt.
4. Når du skal installere sertifikatet, kan du se Installere et Privacy Manager-sertifikat på side 48

Installere et Privacy Manager-sertifikat

1. Når du har mottatt e-postmeldingen med Privacy Manager-sertifikatet vedlagt, åpner du meldingen og klikker på **Setup** (installer) nederst til høyre i meldingen i Outlook 2007, eller øverst til venstre i Outlook 2003.
2. Godkjenn deg med sikkerhetspåloggingsmetoden du har valgt.
3. Klikk på **Neste** på siden Certificate Installed (sertifikat installert).
4. Skriv inn en plassering og et navn på sikkerhetskopifilen på siden Certificate Backup (sikkerhetskopi av sertifikat), eller klikk på **Bla gjennom** for å søke etter en plassering.

△ **FORSIKTIG:** Husk å lagre filen et annet sted enn på harddisken, og legg den et sikkert sted. Denne filen er bare til eget bruk og kreves hvis du må gjenopprette Privacy Manager-sertifikatet og tilhørende nøkler.

5. Skriv inn og bekreft et passord, og klikk deretter på **Neste**.
6. Godkjenn deg med sikkerhetspåloggingsmetoden du har valgt.
7. Hvis du velger å starte invitasjonsprosessen for klarerte kontakter, følger du veiledningen på skjermen fra trinn 2 i emnet Legge til klarerte kontakter via Microsoft Outlook-kontakter på side 52.

   – eller –

Hvis du klikker på **Avbryt**, kan du se Legge til en klarert kontakt på side 51 for å få informasjon om hvordan du legger inn klarerte kontakter senere.

Vise detaljer om Privacy Manager-sertifikater

1. Åpne Privacy Manager (personvern) og klikk på **Certificates** (sertifikater).
2. Klikk på et Privacy Manager-sertifikat.
3. Klikk på **Certificate details** (sertifikatdetaljer).
4. Når du er ferdig med å vise detaljene, klikker du på **OK**.

Fornye et Privacy Manager-sertifikat

Når Privacy Manager-sertifikatet nærmer seg utløpstidspunktet, får du et varsel om at det må fornyes:

1. Åpne Privacy Manager (personvern) og klikk på **Certificates** (sertifikater).
2. Klikk på **Renew certificate** (forny sertifikat).
3. Følg veiledningen på skjermen for å kjøpe et nytt Privacy Manager-sertifikat.

MERK: Fornyelsesprosessen for Privacy Manager-sertifikater erstatter ikke det gamle Privacy Manager-sertifikatet. Du må kjøpe et nytt Privacy Manager-sertifikat og installere det ved å bruke samme fremgangsmåte som i Bestille og installere et Privacy Manager-sertifikat på side 47.

Angi et standardsertifikat for Privacy Manager (personvern)

Bare Privacy Manager-sertifikater vises i Privacy Manager, selv om andre sertifikater fra andre sertifiseringsmyndigheter er installert på datamaskinen.

Hvis du har mer enn ett Privacy Manager-sertifikat på datamaskinen som er installert ved hjelp av Privacy Manager, kan du angi et av dem som standardsertifikat:

1. Åpne Privacy Manager (personvern) og klikk på **Certificates** (sertifikater).
2. Klikk på Privacy Manager-sertifikatet du vil bruke som standardsertifikat, og klikk deretter på **Set default** (angi som standard).
3. Klikk på **OK**.

MERK: Du trenger ikke bruke standardsertifikatet for Privacy Manager (personvern). I de ulike Privacy Manager-funksjonene kan du velge å bruke et hvilket som helst av Privacy Manager-sertifikatene.

Slette et Privacy Manager-sertifikat

Hvis du sletter et Privacy Manager-sertifikat, kan du ikke åpne filer eller vise data som du har kryptert med dette sertifikatet. Hvis du i vanvare sletter et Privacy Manager-sertifikat, kan du gjenopprette det med sikkerhetskopifilen som du opprettet da du installerte sertifikatet. Se Gjenopprette et Privacy Manager-sertifikat på side 50 for å få mer informasjon.

Slik sletter du et Privacy Manager-sertifikat:

1. Åpne Privacy Manager (personvern) og klikk på **Certificates** (sertifikater).
2. Klikk på Privacy Manager-sertifikatet du vil slette og deretter på **Advanced** (avansert).

3. Klikk på **Delete** (slett).
4. Når bekreftelsesdialogboksen åpnes, klikker du på **Yes** (ja).
5. Klikk på **Close** (lukk) og deretter på **Bruk**.

Gjenopprette et Privacy Manager-sertifikat

Ved installering av et Privacy Manager-sertifikat blir du bedt om å lage en sikkerhetskopi av sertifikatet. Du kan også lage en sikkerhetskopi fra migreringssiden. Denne sikkerhetskopien kan brukes ved migrering til en annen datamaskin eller for å gjenopprette sertifikatet på samme datamaskin.

1. Åpne Privacy Manager (personvern) og klikk på **Migration** (migrering).
2. Klikk på **Restore** (gjenopprett).
3. Klikk på **Bla gjennom** på siden Migration File (migreringsfil) for å søke etter .dppsm-filen som du opprettet ved sikkerhetskopiering, og klikk deretter på **Neste**.
4. Oppgi passordet du brukte da du laget sikkerhetskopien, og klikk deretter på **Neste**.
5. Klikk på **Fullfør**.
6. Klikk på **OK**.

Se Installere et Privacy Manager-sertifikat på side 48 eller Sikkerhetskopiere Privacy Manager-sertifikater og klarerte kontakter på side 65 for å få mer informasjon.

Tilbakekalle Privacy Manager-sertifikatet

Hvis du tror sikkerheten til Privacy Manager-sertifikatet er kompromittert, kan du tilbakekalle ditt eget sertifikat:

MERK: Et tilbakekalt Privacy Manager-sertifikat blir ikke slettet. Sertifikatet kan fremdeles brukes til å vise filer som er kryptert.

1. Åpne Privacy Manager (personvern) og klikk på **Certificates** (sertifikater).
2. Klikk på **Advanced** (avansert).
3. Klikk på Privacy Manager-sertifikatet du vil tilbakekalle, og deretter på **Revoke** (tilbakekall).
4. Når bekreftelsesdialogboksen åpnes, klikker du på **Yes** (ja).
5. Godkjenn deg med sikkerhetspåloggingsmetoden du har valgt.
6. Følg veiledningen på skjermen.

Administrere klarerte kontakter

Klarerte kontakter er brukere som du har utvekslet Privacy Manager-sertifikater med, slik at dere kan kommunisere sikkert med hverandre.

Med Trusted Contacts Manager (behandling av klarerte kontakter) kan du utføre følgende oppgaver:

- Vise detaljer om klarerte kontakter
- Slette klarerte kontakter
- Sjekke tilbakekallingsstatus for klarerte kontakter (avansert)

Legge til klarerte kontakter

Det å legge inn klarerte kontakter er en tretrinnsprosess:

1. Du sender en e-postinvitasjon til en klarert kontaktmottaker.
2. Den klarerte kontaktmottakeren svarer på e-postmeldingen.
3. Du mottar et e-postsvar fra den klarerte kontaktmottakeren og klikker på **Accept** (godta).

Du kan sende invitasjon til å bli en klarert kontakt med e-post til enkeltmottakere, eller du kan sende invitasjoner til alle dine kontakter i Microsoft Outlook-adresseboken.

Se de neste avsnittene for å få mer informasjon om å legge til klarerte kontakter.

MERK: For å svare på en invitasjon om å bli en klarert kontakt må den klarerte kontaktmottakeren ha Privacy Manager (personvern) eller en alternativ klient installert på datamaskinen. Hvis du vil ha informasjon om installering av alternative klienter, kan du gå til nettstedet DigitalPersona på http://DigitalPersona.com/PrivacyManager.

Legge til en klarert kontakt

1. Åpne Privacy Manager (personvern) og klikk på **Trusted Contacts Manager** (behandling av klarerte kontakter) og deretter på **Invite Contacts** (inviter kontakter).

   – eller –

   Klikk på nedpilen ved siden av **Send Securely** (send sikkert) på verktøylinjen i Microsoft Outlook, og klikk deretter på **Invite Contacts** (inviter kontakter).

2. Hvis dialogboksen Select Certificate (velg sertifikat) åpnes, klikker du på Privacy Manager-sertifikatet du vil bruke, og deretter på **OK**.

3. Når dialogboksen Trusted Contact Invitation (invitasjon til klarert kontakt) åpnes, leser du teksten og klikker på **OK**.

   Det genereres automatisk en e-postmelding.

4. Skriv inn én eller flere e-postadresser for mottakerne du vil legge inn som klarerte kontakter.

5. Rediger teksten og signer med navnet ditt (valgfritt).

6. Klikk på **Send**.

   MERK: Hvis du ikke har skaffet deg et Privacy Manager-sertifikat, får du melding om at du må ha et Privacy Manager-sertifikat for å sende forespørsler om å bli klarerte kontakter. Klikk på **OK** for å åpne veiviseren for sertifikatforespørsler. Se Bestille og installere et Privacy Manager-sertifikat på side 47 for å få mer informasjon.

7. Godkjenn deg med sikkerhetspåloggingsmetoden du har valgt.

MERK: Når e-postmeldingen mottas av klarert kontaktmottakeren, må han eller hun åpne e-postmeldingen, klikke på **Accept** (godta) nederst til høyre i e-postmeldingen og deretter klikke på **OK** når bekreftelsesdialogboksen åpnes.

8. Når du mottar et e-postsvar fra en mottaker som godtar invitasjonen om å bli en klarert kontakt, klikker du på **Accept** (godta) nederst til høyre i meldingen.

   Det åpnes en dialogboks som bekrefter at mottakeren er lagt til på listen over klarerte kontakter.

9. Klikk på **OK**.

Legge til klarerte kontakter via Microsoft Outlook-kontakter

1. Åpne Privacy Manager (personvern) og klikk på **Trusted Contacts Manager** (behandling av klarerte kontakter) og deretter på **Invite Contacts** (inviter kontakter).

   – eller –

   Klikk på nedpilen ved siden av **Send Securely** (send sikkert) på verktøylinjen i Microsoft Outlook, og klikk deretter på **Invite All My Outlook Contacts** (inviter alle Outlook-kontakter).

2. Når siden Trusted Contact Invitation (invitasjon til klarert kontakt) åpnes, velger du e-postadressene til mottakerne du vil legge inn som klarerte kontakter, og klikker på **Neste**.

3. Når siden Sending Invitation (sender invitasjon) åpnes, klikker du på **Fullfør**.

   Det genereres automatisk en e-postmelding med alle e-postadressene som er valgt i Microsoft Outlook.

4. Rediger teksten og signer med navnet ditt (valgfritt).

5. Klikk på **Send**.

MERK: Hvis du ikke har skaffet deg et Privacy Manager-sertifikat, får du melding om at du må ha et Privacy Manager-sertifikat for å sende forespørsler om å bli klarerte kontakter. Klikk på **OK** for å åpne veiviseren for sertifikatforespørsler. Se Bestille og installere et Privacy Manager-sertifikat på side 47 for å få mer informasjon.

6. Godkjenn deg med sikkerhetspåloggingsmetoden du har valgt.

MERK: Når e-postmeldingen mottas av klarert kontaktmottakeren, må han eller hun åpne e-postmeldingen, klikke på **Accept** (godta) nederst til høyre i e-postmeldingen og deretter klikke på **OK** når bekreftelsesdialogboksen åpnes.

7. Når du mottar et e-postsvar fra en mottaker som godtar invitasjonen om å bli en klarert kontakt, klikker du på **Accept** (godta) nederst til høyre i meldingen.

   Det åpnes en dialogboks som bekrefter at mottakeren er lagt til på listen over klarerte kontakter.

8. Klikk på **OK**.

Vise detaljer om klarerte kontakter

1. Åpne Privacy Manager (personvern) og klikk på **Trusted Contacts** (klarerte kontakter).

2. Klikk på en klarert kontakt.

3. Klikk på **Contact details** (kontaktdetaljer).
4. Når du er ferdig med å vise detaljene, klikker du på **OK**.

Slette en klarert kontakt

1. Åpne Privacy Manager (personvern) og klikk på **Trusted Contacts** (klarerte kontakter).
2. Klikk på den klarerte kontakten du vil slette.
3. Klikk på **Delete contact** (slett kontakt).
4. Når bekreftelsesdialogboksen åpnes, klikker du på **Yes** (ja).

Sjekke tilbakekallingsstatus for en klarert kontakt

Slik ser du om en klarert kontakt har tilbakekalt Privacy Manager-sertifikatet sitt:

1. Åpne Privacy Manager (personvern) og klikk på **Trusted Contacts** (klarerte kontakter).
2. Klikk på en klarert kontakt.
3. Klikk på **Advanced** (avansert).

   Dialogboksen Advanced Trusted Contact Management (avansert behandling av klarerte kontakter) åpnes.
4. Klikk på **Check Revocation** (sjekk tilbakekalling).
5. Klikk på **Lukk**.

Generelle oppgaver

Du kan bruke Privacy Manager (personvern) sammen med disse Microsoft-produktene:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Bruke Privacy Manager (personvern) i Microsoft Outlook

Når Privacy Manager (personvern) er installert, vises knappen Privacy (personvern) på verktøylinjen i Microsoft Outlook, og knappen Send Securely (send sikkert) vises på verktøylinjen til alle e-postmeldinger i Microsoft Outlook. Når du klikker på nedpilen ved siden av **Privacy** (personvern) eller **Send Securely** (send sikkert), får du disse valgmulighetene:

- Sign and Send (signer og send, kun Send Securely-knapp) – Dette alternativet legger til en digital signatur i e-postmeldingen og sender meldingen når du har godkjent deg med den valgte sikkerhetspåloggingsmetoden.
- Seal for Trusted Contacts and Send (forsegl for klarerte kontakter og send, kun Send Securely-knapp) – Dette alternativet legger til en digital signatur i e-postmeldingen, krypterer meldingen og sender den når du har godkjent deg med den valgte sikkerhetspåloggingsmetoden.
- Invite Contacts (inviter kontakter) – Dette alternativet gir deg mulighet til å sende en invitasjon om å bli en klarert kontakt. Se Legge til en klarert kontakt på side 51 for å få mer informasjon.
- Invite Outlook Contacts (inviter Outlook-kontakter) – Dette alternativet gir deg mulighet til å sende en invitasjon om å bli klarerte kontakter til alle kontakter i Microsoft Outlook-adresseboken. Se Legge til klarerte kontakter via Microsoft Outlook-kontakter på side 52 for å få mer informasjon.
- Open the Privacy Manager software (åpne Privacy Manager-programvaren) – Alternativer for sertifikater, klarerte kontakter og innstillinger gir deg mulighet til å åpne Privacy Manager-programvaren for å legge til, vise eller endre gjeldende innstillinger. Se Konfigurere Privacy Manager (personvern) for Microsoft Outlook på side 54 for å få mer informasjon.

Konfigurere Privacy Manager (personvern) for Microsoft Outlook

1. Åpne Privacy Manager (personvern) og klikk på **Settings** (innstillinger) og deretter på kategorien **E-Mail** (e-post).

   – eller –

   Klikk på nedpilen ved siden av **Send Securely** (send sikkert), (**Privacy** (privat) i Outlook 2003) på verktøylinjen i Microsoft Outlook, og klikk deretter på **Settings** (innstillinger).

   – eller –

   Klikk på nedpilen ved siden av **Send Securely** (send sikkert) på verktøylinjen i en e-postmelding, og klikk deretter på **Settings** (innstillinger).

2. Velg handlingene du vil utføre når du sender sikker e-post, og klikk deretter på **OK**.

Signere og sende en e-postmelding

1. Klikk på **Ny** eller **Svar** i Microsoft Outlook.
2. Skriv e-postmeldingen.
3. Klikk på nedpilen ved siden av **Send Securely** (send sikkert), (**Privacy** (privat) i Outlook 2003), og klikk deretter på **Sign and Send** (signer og send).
4. Godkjenn deg med sikkerhetspåloggingsmetoden du har valgt.

Forsegle og sende en e-postmelding

Forseglede e-postmeldinger som er digitalt signert og forseglet (kryptert), kan bare vises av dem du velger ut på listen over klarerte kontakter.

Slik forsegler og sender du en e-postinvitasjon til en klarert kontakt:

1. Klikk på **Ny** eller **Svar** i Microsoft Outlook.
2. Skriv e-postmeldingen.
3. Klikk på nedpilen ved siden av **Send Securely** (send sikkert), (**Privacy** (privat) i Outlook 2003), og klikk deretter på **Seal for Trusted Contacts and Send** (forsegl for klarerte kontakter og send).
4. Godkjenn deg med sikkerhetspåloggingsmetoden du har valgt.

Vise en forseglet e-postmelding

Når du åpner en forseglet e-postmelding, vises sikkerhetsmerket i overskriften til e-postmeldingen. Sikkerhetsmerket inneholder følgende informasjon:

- Påloggingsinformasjonen som ble brukt til å bekrefte identiteten til personen som signerte e-postmeldingen
- Produktet som ble brukt til å bekrefte påloggingsinformasjonen til personen som signerte e-postmeldingen

Bruke Privacy Manager (personvern) i et Microsoft Office-dokument

MERK: Privacy Manager (personvern) kan bare brukes sammen med Microsoft Office 2007-dokumenter.

Når du har installert et Privacy Manager-sertifikat, vises knappen Sign and Encrypt (signer og krypter) til høyre på verktøylinjen i alle Microsoft Word-, Microsoft Excel- og Microsoft PowerPoint-dokumenter. Når du klikker på nedpilen ved siden av **Sign and Encrypt** (signer og krypter), får du disse valgmulighetene:

- Sign Document (signer dokument) – Dette alternativet legger til din digitale signatur i dokumentet.
- Add Signature Line Before Signing (legg til signaturlinje før signering, kun Microsoft Word og Microsoft Excel) – Som standard blir en signaturlinje lagt til når et Microsoft Word- eller Microsoft Excel-dokument blir signert eller kryptert. Du slår av dette alternativet ved å klikke på **Add Signature Line** (legg til signaturlinje) for å oppheve merkingen.
- Encrypt Document (krypter dokument) – Dette alternativet legger til din digitale signatur i dokumentet og krypterer det.

- Remove Encryption (fjern kryptering) – Dette alternativet fjerner krypteringen av dokumentet.
- Open the Privacy Manager software (åpne Privacy Manager-programvaren) – Alternativer for sertifikater, klarerte kontakter og innstillinger gir deg mulighet til å åpne Privacy Manager-programvaren for å legge til, vise eller endre gjeldende innstillinger. Se Administrere Privacy Manager-sertifikater på side 47, Administrere klarerte kontakter på side 50 eller Konfigurere Privacy Manager (personvern) for Microsoft Office på side 56 for å få mer informasjon.

Konfigurere Privacy Manager (personvern) for Microsoft Office

1. Åpne Privacy Manager (personvern) og klikk på **Settings** (innstillinger) og deretter på kategorien **Documents** (dokumenter).

   – eller –

   Klikk på nedpilen ved siden av **Sign and Encrypt** (signer og krypter) på verktøylinjen i et Microsoft Office-dokument, og klikk deretter på **Settings** (innstillinger).

2. Velg handlingene du vil konfigurere, og klikk deretter på **OK**.

Signere et Microsoft Office-dokument

1. Opprett og lagre et dokument i Microsoft Word, Microsoft Excel eller Microsoft PowerPoint.
2. Klikk på nedpilen ved siden av **Sign and Encrypt** (signer og krypter) og deretter på **Sign Document** (signer dokument).
3. Godkjenn deg med sikkerhetspåloggingsmetoden du har valgt.
4. Når bekreftelsesdialogboksen åpnes, leser du teksten og klikker på **OK**.

Følg denne fremgangsmåten hvis du senere vil redigere dokumentet:

1. Klikk på **Office**-knappen øverst til høyre på skjermbildet.
2. Klikk på **Prepare** (klargjør) og deretter på **Mark as Final** (merk som endelig).
3. Når bekreftelsesdialogboksen åpnes, klikker du på **Yes** (ja) og fortsetter arbeidet.
4. Når du har fullført redigeringen, signerer du dokumentet på nytt.

Legge til signaturlinje når du signerer et Microsoft Word- eller Microsoft Excel-dokument

Du kan legge til en signaturlinje i Privacy Manager (personvern) når du signerer et Microsoft Word- eller Microsoft Excel-dokument:

1. Opprett og lagre et dokument i Microsoft Word eller Microsoft Excel.
2. Klikk på menyen **Home** (hjem).
3. Klikk på nedpilen ved siden av **Sign and Encrypt** (signer og krypter) og deretter på **Add Signature Line Before Signing** (legg til signaturlinje før signering).

MERK: Det vises en hake ved siden av Add Signature Line Before Signing (legg til signaturlinje før signering) når dette alternativet velges. Dette alternativet er som standard aktivert.

4. Klikk på nedpilen ved siden av **Sign and Encrypt** (signer og krypter) og deretter på **Sign Document** (signer dokument).

5. Godkjenn deg med sikkerhetspåloggingsmetoden du har valgt.

Legge til foreslåtte undertegnere i et Microsoft Word- eller Microsoft Excel-dokument

Du kan legge til mer enn én signaturlinje i et dokument ved å utpeke foreslåtte undertegnere. En foreslått undertegner er en bruker som er utpekt av eieren av et Microsoft Word- eller Microsoft Excel-dokument til å legge til en signaturlinje i dokumentet. Foreslåtte undertegnere kan være du eller en annen person du vil at skal signere dokumentet. Hvis du for eksempel klargjør et dokument som må signeres av alle i avdelingen, kan du inkludere signaturlinjer for disse brukerne nederst på siste side av dokumentet med instruksjon om at de må signere innen en bestemt dato.

Slik legger du til foreslåtte undertegnere i et Microsoft Word- eller Microsoft Excel-dokument:

1. Opprett og lagre et dokument i Microsoft Word eller Microsoft Excel.

2. Klikk på menyen **Insert** (sett inn).

3. I gruppen **Text** (tekst) på verktøylinjen klikker du på pilen ved siden av **Signature Line** (signaturlinje) og deretter på **Privacy Manager Signature Provider** (signaturtjeneste).

   Dialogboksen Signature Setup (signaturoppsett) åpnes.

4. I tekstboksen under **Suggested signer** (foreslått undertegner) skriver du inn navnet på den foreslåtte undertegneren.

5. I tekstboksen under **Instructions to the signer** (instruksjoner til undertegner) skriver du inn en melding til den foreslåtte undertegneren.

   MERK: Denne meldingen vises i stedet for en tittel og kan slettes eller byttes ut med brukerens tittel når dokumentet signeres.

6. Merk av for **Show sign date in signature line** (vis signeringsdato på signaturlinjen) for å vise datoen.

7. Merk av for **Show signer's title in signature line** (vis undertegners tittel på signaturlinjen) for å vise tittelen.

   MERK: I og med at eieren av dokumentet utpeker foreslåtte undertegnere til dokumentet, kan ikke den foreslåtte undertegneren vise datoen og/eller tittelen hvis det ikke er merket av for **Show sign date in signature line** (vis signeringsdato på signaturlinjen) og/eller **Show signer's title in signature line** (vis undertegners tittel på signaturlinjen), selv om den foreslåtte undertegnerens dokumentinnstillinger er konfigurert for å gjøre dette.

8. Klikk på **OK**.

Legge til en foreslått undertegners signaturlinje

Når de foreslåtte undertegnerne åpner dokumentet, vises navnet deres i parentes for å angi at en signatur er nødvendig.

Slik signeres dokumentet:

1. Dobbeltklikk på den aktuelle signaturlinjen.

2. Godkjenn deg med sikkerhetspåloggingsmetoden du har valgt.

Signaturlinjen vises i henhold til innstillingene som er angitt av eieren av dokumentet.

Kryptere et Microsoft Office-dokument

Du kan kryptere et Microsoft Office-dokument for deg selv og klarerte kontakter. Når du krypterer et dokument og lukker det, må du og klarerte kontakter du velger fra listen, godkjennes før det kan åpnes.

Slik krypterer du et Microsoft Office-dokument:

1. Opprett og lagre et dokument i Microsoft Word, Microsoft Excel eller Microsoft PowerPoint.
2. Klikk på menyen **Home** (hjem).
3. Klikk på nedpilen ved siden av **Sign and Encrypt** (signer og krypter) og deretter på **Encrypt Document** (krypter dokument).

   Dialogboksen Select Trusted Contacts (velg klarerte kontakter) åpnes.
4. Klikk på navnet til en klarert kontakt som skal kunne åpne dokumentet og vise innholdet.

   MERK: Hvis du vil velge navnene på flere klarerte kontakter, holder du nede ctrl-tasten og klikker på de enkelte navnene.
5. Klikk på **OK**.

Følg fremgangsmåten i Fjerne krypteringen av et Microsoft Office-dokument på side 58 hvis du senere vil redigere dokumentet. Når krypteringen er fjernet, kan du redigere dokumentet. Følg fremgangsmåten i dette avsnittet for å kryptere dokumentet igjen.

Fjerne krypteringen av et Microsoft Office-dokument

Når du fjerner krypteringen fra et Microsoft Office-dokument, kreves det ikke lenger at du eller klarerte kontakter godkjennes før dere kan åpne og vise innholdet i dokumentet.

Slik fjerner du krypteringen av et Microsoft Office-dokument:

1. Åpne et kryptert dokument i Microsoft Word, Microsoft Excel eller Microsoft PowerPoint.
2. Godkjenn deg med sikkerhetspåloggingsmetoden du har valgt.
3. Klikk på menyen **Home** (hjem).
4. Klikk på nedpilen ved siden av **Sign and Encrypt** (signer og krypter) og deretter på **Remove Encryption** (fjern kryptering).

Sende et kryptert Microsoft Office-dokument

Du kan legge et kryptert Microsoft Office-dokument ved en e-postmelding uten å signere eller kryptere selve e-postmeldingen. Det gjør du ved å opprette og sende en e-postmelding med et signert eller kryptert dokument vedlagt, slik du normalt gjør med en e-postmelding med vedlegg.

For å få optimal sikkerhet anbefales det imidlertid at du krypterer e-postmeldingen når du legger ved et signert eller kryptert Microsoft Office-dokument.

Følg denne fremgangsmåten for å sende en forseglet e-postmelding med et vedlagt signert og/eller kryptert Microsoft Office-dokument:

1. Klikk på **Ny** eller **Svar** i Microsoft Outlook.
2. Skriv e-postmeldingen.
3. Legg ved Microsoft Office-dokumentet.
4. Se Forsegle og sende en e-postmelding på side 55 for å få ytterligere veiledning.

Vise et signert Microsoft Office-dokument

MERK: Du trenger ikke å ha et Privacy Manager-sertifikat for å vise et signert Microsoft Office-dokument.

Når et signert Microsoft Office-dokument åpnes, vises et ikon for digital signatur på statuslinjen nederst i dokumentvinduet.

1. Klikk på ikonet **Digital Signatures** (digitale signaturer) for å vise eller skjule signaturdialogboksen, som viser navnet på alle brukere som har signert dokumentet, og hvilken dato de gjorde det.
2. Høyreklikk på et navn i signaturdialogboksen og velg Signature Details (signaturdetaljer) for å vise flere detaljer om hver enkelt signatur.

Vise et kryptert Microsoft Office-dokument

Hvis et kryptert Microsoft Office-dokument skal vises på en annen datamaskin, må Privacy Manager (personvern) være installert på denne datamaskinen. I tillegg må du gjenopprette Privacy Manager-sertifikatet som ble brukt til å kryptere filen.

En klarert kontakt som vil vise et kryptert Microsoft Office-dokument, må ha et Privacy Manager-sertifikat og Privacy Manager må være installert på datamaskinen. I tillegg må den klarerte kontakten velges av eieren av det krypterte Microsoft Office-dokumentet.

Bruke Privacy Manager (personvern) i Windows Live Messenger

Privacy Manager (personvern) legger til følgende sikre kommunikasjonsfunksjoner i Windows Live Messenger:

- **Secure chat** (sikker chatting) – Meldinger sendes med SSL/TLS (Secure Sockets Layer/Transport Layer Security) via XML-protokollen, den samme teknologien som sørger for sikkerheten når det gjelder e-handelstransaksjoner.
- **Recipient identification** (mottakeridentifikasjon) – Du kan bekrefte nærværet og identiteten til en person før du sender en melding.
- **Signed messages** (signerte meldinger) – Du kan signere meldinger elektronisk. Hvis meldingen er endret eller tuklet med, blir den merket som ugyldig når mottakeren mottar den.
- **Hide/show feature** (skjul/vis funksjon) – Du kan vise eller skjule hvilke som helst eller alle meldingene i chattevinduet til Privacy Manager (personvern). Du kan også sende en melding der innholdet er skjult. Da kreves godkjenning før meldingen vises.

- **Secure chat history** (sikker chattelogg) – Logger over chatteøkter krypteres før de lagres og det kreves godkjenning for å se på dem.
- **Automatic locking/unlocking** (automatisk låsing/opplåsing) – Du kan låse og låse opp chattevinduet til Privacy Manager (personvern) eller angi at det skal låses automatisk etter en angitt periode med uvirksomhet.

Starte en chatteøkt i Privacy Manager (personvern)

MERK: For å kunne bruke Privacy Manager-chatting må begge parter ha Privacy Manager (personvern) og et Privacy Manager-sertifikat installert. Se Bestille og installere et Privacy Manager-sertifikat på side 47 for å få mer informasjon om installering av Privacy Manager-sertifikater.

1. Bruk en av følgende fremgangsmåter for å starte Privacy Manager-chatting i Windows Live Messenger:

   a. Høyreklikk på en nettkontakt i Live Messenger, og velg deretter **Start en aktivitet**.

   b. Klikk på **Start Chat** (start chatting).

   – eller –

   a. Dobbeltklikk på en nettkontakt i Live Messenger og klikk deretter på menyen **Vis en liste over aktiviteter**.

   b. Klikk på **Handling** og deretter på **Start Chat** (start chatting).

   – eller –

   a. Høyreklikk på **ProtectTools**-ikonet i systemstatusfeltet, klikk på **Privacy Manager for HP ProtectTools** (personvern) og velg **Start Chat** (start chatting).

   b. I Live Messenger klikker du på **Handlinger: Start en aktivitet** og velger **Privacy Manager Chat** (chatting).

   MERK: Hver bruker må være på nettet i Live Messenger og brukerne må vises i hverandres Live Messenger-nettvindu. Klikk for å velge en bruker på nettet.

   Privacy Manager (personvern) sender en invitasjon til kontakten om å starte Privacy Manager Chat (chatting). Når den inviterte kontakten godtar invitasjonen, åpnes vinduet Privacy Manager Chat (chatting). Hvis den inviterte kontakten ikke har Privacy Manager (personvern), blir han eller hun bedt om å laste ned programmet.

2. Klikk på **Start** for å innlede en sikker chatteøkt.

Konfigurere Privacy Manager (personvern) for Windows Live Messenger

1. Klikk på **Settings** (innstillinger) i Privacy Manager Chat (chatting).

   – eller –

   Klikk på **Settings** (nnstillinger) i Privacy Manager (personvern) og deretter på kategorien **Chat** (chatting).

   – eller –

   Klikk på **Settings** (innstillinger) i Privacy Manager Live Messenger History Viewer (loggvisning).

2. For å angi hvor lenge Privacy Manager Chat (chatting) skal vente før en økt låses, velger du et tall fra listen **Lock session after _ minutes of inactivity** (lås økt etter _ minutter uten aktivitet).

3. Hvis du vil angi en loggmappe for chatteøktene, klikker du på **Bla gjennom** for å søke etter mappen, og deretter klikker du på **OK**.

4. Hvis du vil at øktene skal krypteres og lagres automatisk når du lukker dem, merker du av for **Automatically save secure chat history** (lagre sikker chattelogg automatisk).

5. Klikk på **OK**.

Chatte i vinduet Privacy Manager Chat (chatting)

Når du har startet Privacy Manager Chat (chatting), åpnes vinduet Privacy Manager Chat (chatting) i Windows Live Messenger. Privacy Manager Chat (chatting) likner mye på grunnleggende bruk av Windows Live Messenger, bortsett fra at følgende tilleggsfunksjoner er tilgjengelig i vinduet Privacy Manager Chat (chatting):

- **Save** (lagre) – Klikk på denne knappen for å lagre chatteøkten i mappen du valgte i konfigurasjonsinnstillingene. Du kan også konfigurere Privacy Manager Chat (chatting) for automatisk å lagre hver økt når den lukkes.
- **Hide all** (skjul alle) og **Show all** (vis alle) – Klikk på den aktuelle knappen for å utvide eller skjule meldingene som vises i vinduet Secure Communications (sikker kommunikasjon). Du kan også skjule eller vise enkeltmeldinger ved å klikke på meldingshodet.
- **Are you there?** (Er du der?) – Klikk på denne knappen for å be om godkjenning av kontakten.
- **Lock** (lås) – Klikk på denne knappen for å lukke vinduet Privacy Manager Chat (chatting) og gå tilbake til vinduet Chat Entry (chatteregistrering). Hvis du vil vise vinduet Secure Communications (sikker kommunikasjon) igjen, klikker du på **Resume the session** (fortsett økten) og godkjenner deg med sikkerhetspåloggingsmetoden du har valgt.
- **Send** – Klikk på denne knappen for å sende en kryptert melding til kontakten.
- **Send signed** (send signert) – Merk av for dette for å signere og kryptere meldingene elektronisk. Hvis en melding er endret eller tuklet med, blir den merket som ugyldig når mottakeren mottar den. Du må godkjenne deg hver gang du sender en signert melding.
- **Send hidden** (send skjult) – Merk av for dette for å kryptere og sende en melding som viser bare meldingshodet. Kontakten må godkjenne seg for å lese innholdet i meldingen.

Vise chattelogg

Privacy Manager Chat: Live Messenger History Viewer (loggvisning) viser krypterte filer med Privacy Manager Chat-økter. Øktene kan lagres ved å klikke på **Save** (lagre) i vinduet Privacy Manager Chat

(chatting) eller ved å konfigurere automatisk lagring i kategorien Chat (chatting) i Privacy Manager (personvern). Hver økt vises med det (krypterte) skjermnavnet til kontakten og datoen og klokkeslettet da økten startet og sluttet. Som standard vises alle økter for alle e-postkonti du har konfigurert. Du kan bruke menyen **Display history for** (vis logg for) til å velge ut bestemte konti for visning.

Ved loggvisning kan du utføre følgende oppgaver:

- Avdekke alle økter på side 62
- Avdekke øktene for en bestemt konto på side 62
- Vise en økt-ID på side 63
- Vise en økt på side 63
- Søke etter bestemt tekst i økter på side 63
- Slette en økt på side 63
- Legge til eller fjerne kolonner på side 63
- Filtrere øktene som vises på side 64

Slik starter du Live Messenger History Viewer (loggvisning):

▲ Høyreklikk på **HP ProtectTools**-ikonet i systemstatusfeltet helt til høyre på oppgavelinjen, klikk på **Privacy Manager: for HP ProtectTools** (personvern) og klikk deretter på **Live Messenger History Viewer** (loggvisning).

– eller –

▲ Klikk på **History Viewer** (loggvisning) eller **History** (logg) i en chatteøkt.

Avdekke alle økter

Avdekking av alle økter viser det dekrypterte skjermnavnet til kontakten for den eller de valgte øktene og alle øktene for samme konto.

Slik avdekker du alle lagrede chatteloggøkter:

1. Høyreklikk på en økt i Live Messenger History Viewer (loggvisning) og velg **Reveal All Sessions** (avdekk alle økter).
2. Godkjenn deg med sikkerhetspåloggingsmetoden du har valgt.

   Skjermnavnene til kontaktene dekrypteres.
3. Dobbeltklikk på en økt for å vise innholdet.

Avdekke øktene for en bestemt konto

Avdekking av en økt viser det dekrypterte skjermnavnet til kontakten for den valgte økten.

Slik avdekker du en bestemte chatteloggøkt:

1. Høyreklikk på en økt i Live Messenger History Viewer (loggvisning) og velg **Reveal Session** (avdekk økt).
2. Godkjenn deg med sikkerhetspåloggingsmetoden du har valgt.

   Skjermnavnet til kontakten dekrypteres.
3. Dobbeltklikk på den avdekkete økten for å vise innholdet.

MERK: Andre økter som er kryptert med samme sertifikat, viser et opplåst ikon for å angi at du kan vise dem ved å dobbeltklikke på en av øktene uten ytterligere godkjenning. Økter som er kryptert med et annet sertifikat, viser et låst ikon for å angi at ytterligere godkjenning kreves for disse øktene før du kan vise skjermnavnene til kontaktene eller innholdet.

Vise en økt-ID

Slik viser du en økt-ID:

- Høyreklikk på en avdekket økt i Live Messenger History Viewer (loggvisning) og velg **View** (vis).

Vise en økt

Visning av en økt åpner filen for visning. Hvis økten ikke er avdekket fra før (viser det krypterte skjermnavnet til kontakten), avdekkes den samtidig.

Slik viser du en Live Messenger-loggøkt:

1. Høyreklikk på en økt i Live Messenger History Viewer (loggvisning) og velg **View** (vis).
2. Godkjenn deg med sikkerhetspåloggingsmetoden du har valgt, hvis du blir bedt om det.

   Innholdet i økten dekrypteres.

Søke etter bestemt tekst i økter

Du kan søke etter tekst bare i avdekkete (dekrypterte) økter som vises i visningsvinduet. Dette er øktene der skjermnavnene til kontaktene vises som vanlig tekst.

Slik søker du etter tekst i chatteloggøkter:

1. Klikk på **Search** (søk) i Live Messenger History Viewer (loggvisning).
2. Skriv inn søketeksten, konfigurer eventuelle søkeparametere og klikk på **OK**.

   Økter som inneholder teksten, utheves i visningsvinduet.

Slette en økt

1. Velg en chatteloggøkt.
2. Klikk på **Delete** (slett).

Legge til eller fjerne kolonner

Som standard vises de tre mest brukte kolonnene i Live Messenger History Viewer (loggvisning). Du kan legge til flere kolonner i visningen, eller du kan fjerne kolonner.

Slik legger du til kolonner:

1. Høyreklikk på en kolonneoverskrift og velg **Add/Remove Columns** (legg til/fjern kolonner).
2. Velg en kolonneoverskrift i venstre panel og klikk på **Add** (legg til) for å flytte den til høyre panel.

Slik fjerner du kolonner:

1. Høyreklikk på en kolonneoverskrift og velg **Add/Remove Columns** (legg til/fjern kolonner).
2. Velg en kolonneoverskrift i høyre panel og klikk på **Remove** (fjern) for å flytte den til venstre panel.

Filtrere øktene som vises

En liste over økter for alle konti vises i Live Messenger History Viewer (loggvisning). Du kan også filtrere øktene ut fra følgende kriterier:

- Bestemte konto. Se Vise økter for en bestemt konto på side 64 for å få mer informasjon.
- Tidsrom. Se Vise økter for en tidsperiode på side 64 for å få mer informasjon.
- Ulike mapper. Se Vise økter som er lagret i en annen mappe enn standardmappen på side 64 for å få mer informasjon.

Vise økter for en bestemt konto

▲ Velg en økt fra menyen **Display history for** (vis logg for) i Live Messenger History Viewer (loggvisning).

Vise økter for en tidsperiode

1. Klikk på ikonet **Advanced Filter** (avansert filter) i Live Messenger History Viewer (loggvisning).

   Dialogboksen Advanced Filter (avansert filter) åpnes.

2. Merk av for **Display only sessions within specified date range** (vis bare økter innen angitt tidsrom).
3. I tekstboksene **From date** (fra dato) og **To date** (til dato) skriver du inn dag, måned og/eller år, eller klikker på pilen ved siden av kalenderen for å velge datoer.
4. Klikk på **OK**.

Vise økter som er lagret i en annen mappe enn standardmappen

1. Klikk på ikonet **Advanced Filter** (avansert filter) i Live Messenger History Viewer (loggvisning).
2. Merk av for **Use an alternate history files folder** (bruk en alternativ loggfilmappe).
3. Oppgi mappeplasseringen eller klikk på **Bla gjennom** for å søke etter en mappe.
4. Klikk på **OK**.

Avanserte oppgaver

Migrere sertifikater for Privacy Manager (personvern) og klarerte kontakter til en annen datamaskin

Du kan migrere Privacy Manager-sertifikater og klarerte kontakter til en annen datamaskin på en sikker måte, eller sikkerhetskopiere data for trygg oppbevaring. Det gjør du ved å sikkerhetskopiere data som en passordbeskyttet fil til en nettverksplassering eller en annen flyttbar lagringsenhet, og deretter gjenopprette filen på den nye datamaskinen.

Sikkerhetskopiere Privacy Manager-sertifikater og klarerte kontakter

Slik sikkerhetskopierer du Privacy Manager-sertifikater og klarerte kontakter til en passordbeskyttet fil:

1. Åpne Privacy Manager (personvern) og klikk på **Migration** (migrering).
2. Klikk på **Backup** (sikkerhetskopier).
3. På siden Select Data (velg data) velger du datakategoriene som skal tas med i migreringsfilen, og klikker på **Neste**.
4. På siden Migration File (migreringsfil) skriver du inn et filnavn eller klikker på **Bla gjennom** for å søke etter en plassering, og klikker deretter på **Neste**.
5. Skriv inn og bekreft et passord, og klikk deretter på **Neste**.

MERK: Oppbevar dette passordet på et trygt sted. Du trenger det når du skal gjenopprette migreringsfilen.

6. Godkjenn deg med sikkerhetspåloggingsmetoden du har valgt.
7. Klikk på **Fullfør** på siden Migration File Saved (migreringsfil lagret).

Gjenopprette Privacy Manager-sertifikater og klarerte kontakter

Følg denne fremgangsmåten for å gjenopprette Privacy Manager-sertifikater og klarerte kontakter på samme datamaskin eller på en annen datamaskin som ledd i en migreringsprosess:

1. Åpne Privacy Manager (personvern) og klikk på **Migration** (migrering).
2. Klikk på **Restore** (gjenopprett).
3. På siden Migration File (migreringsfil) klikker på **Bla gjennom** for å søke etter filen, og klikker deretter på **Neste**.
4. Oppgi passordet du brukte da du laget sikkerhetskopifilen, og klikk deretter på **Neste**.
5. Klikk på **Fullfør** på siden Migration File (migreringsfil).

Sentral administrasjon av Privacy Manager (personvern)

Din installasjon av Privacy Manager (personvern) kan være del av en sentral installasjon som er tilpasset av administratoren. En eller flere av disse funksjonene kan være aktivert eller deaktivert:

- **Certificate use policy** (sertifikatpolicy) – Du kan være begrenset til å bruke Privacy Manager-sertifikater utstedt av Comodo, eller du kan få lov til å bruke digitale sertifikater som er utstedt av andre sertifiseringsmyndigheter.
- **Encryption policy** (krypteringspolicy) – Krypteringsfunksjonene kan være aktivert eller deaktivert enkeltvis i Microsoft Office eller Outlook og i Windows Live Messenger.

10 File Sanitizer (filrensing) for HP ProtectTools

File Sanitizer (filrensing) er et verktøy som du kan bruke til sikker makulering av digitale aktiva (personlige opplysninger eller filer, historisk eller webrelatert innhold og andre datakomponenter) på datamaskinen og fra tid til annen "bleke" harddisken.

MERK: Denne versjonen av File Sanitizer (filrensing) støtter bare systemets harddisk.

Makulering

Makulering skiller seg fra vanlig Windows®-sletting (også kalt enkel sletting i File Sanitizer (filrensing)) ved at når du makulerer aktiva med File Sanitizer, aktiveres en algoritme som skjuler dataene, slik at det blir praktisk talt umulig å hente frem igjen det opprinnelige innholdet. En enkel Windows-sletting kan etterlate filer (eller aktiva) intakt på harddisken eller i en tilstand der filene (eller aktiva) kan gjenopprettes ved hjelp av rettsvitenskapelige metoder.

Når du velger en makuleringsprofil (High Security, Medium Security eller Low Security (høy, middels eller lav sikkerhet)), velges automatisk en forhåndsdefinert liste over aktiva og en slettemetode for makuleringen. Du kan også lage en egendefinert makuleringsprofil, slik at du kan angi antall makuleringssykluser, hvilke aktiva som skal tas med i makuleringen, hvilke aktiva som skal bekreftes før makulering, og hvilke aktiva som skal utelukkes fra makuleringen. Se Velge eller opprette en makuleringsprofil på side 71 for å få mer informasjon.

Du kan sette opp en plan for automatisk makulering, og du kan også makulere aktiva manuelt når du måtte ønske det. Se Sette opp en makuleringsplan på side 70, Makulere enkeltaktiva manuelt på side 75 eller Makulere alle valgte elementer manuelt på side 75 for å få mer informasjon.

MERK: .dll-filer makuleres og fjernes fra systemet bare hvis de er flyttet til papirkurven.

Bleking av ledig plass

Det å slette aktiva i Windows fjerner ikke innholdet i aktiva fullstendig fra harddisken. Windows sletter bare referansen til aktiva. Innholdet blir liggende på harddisken til andre aktiva overskriver det samme området på harddisken med ny informasjon.

Ved bleking av ledig plass skriver du vilkårlige data over slettede aktiva slik at du på en sikker måte unngår at brukere kan se det opprinnelige innholdet i slettede aktiva.

MERK: Bleking av ledig plass er aktuelt for aktiva som du sletter ved hjelp av Windows Papirkurv, og for aktiva som du sletter manuelt. Bleking av ledig plass gjør ikke makulerte aktiva sikrere.

Du kan angi en plan for automatisk bleking av ledig plass, eller du kan aktivere bleking av ledig plass manuelt via **HP ProtectTools-ikonet** i systemstatusfeltet helt til høyre på oppgavelinjen. Se Sette opp en plan for bleking av ledig plass på side 71 eller Aktivere bleking av ledig plass manuelt på side 76 for å få mer informasjon.

Konfigureringsprosedyrer

Åpne File Sanitizer (filrensing)

Slik åpner du File Sanitizer (filrensing):

1. Klikk på **Start**, **Alle programmer**, **HP** og deretter på **HP ProtectTools Security Manager**.
2. Klikk på **File Sanitizer** (filrensing).

– eller –

▲ Dobbeltklikk på ikonet **File Sanitizer** (filrensing) på skrivebordet.

– eller –

▲ Høyreklikk på **HP ProtectTools**-ikonet i systemstatusfeltet helt til høyre på oppgavelinjen, og klikk på **File Sanitizer** (filrensing) og deretter på **Open File Sanitizer** (åpne filrensing).

Sette opp en makuleringsplan

MERK: Se Velge eller opprette en makuleringsprofil på side 71 for å få informasjon om forhåndsdefinerte makuleringsprofiler eller det å lage en makuleringsprofil.

MERK: Se Makulere enkeltaktiva manuelt på side 75 for å få informasjon om manuell makulering av aktiva.

1. Åpne File Sanitizer (filrensing) og klikk på **Shred** (makuler).
2. Velg et makuleringsalternativ:
   - **Windows shutdown** (avslutning av Windows) – Velg dette alternativet hvis du vil makulere alle valgte aktiva når Windows avsluttes.

     MERK: Hvis du velger dette alternativet, åpnes det en dialogboks ved avslutning og spør om du vil fortsette med makulering av valgte aktiva eller om du vil hoppe over prosedyren. Klikk på **Yes** (ja) for å hoppe over makuleringen, eller klikk på **No** (nei) for å fortsette makuleringen.
   - **Web browser open** (åpning av nettleser) – Velg dette alternativet for å makulere alle nettrelaterte aktiva, som nettleserens URL-logg, når du åpner en nettleser.
   - **Web browser quit** (avslutning av nettleser) – Velg dette alternativet for å makulere alle nettrelaterte aktiva, som nettleserens URL-logg, når du lukker en nettleser.
   - **Key sequence** (tastsekvens) – Velg dette alternativet for å starte makulering med en tastsekvens.
   - **Scheduler** (planlegger) – Merk av for **Activate Scheduler** (aktiv planlegger), skriv inn Windows-passordet og oppgi dag og klokkeslett for makulering av valgte aktiva.

   MERK: .dll-filer makuleres og fjernes fra systemet bare hvis de er flyttet til papirkurven.
3. Klikk på **Bruk** og deretter på **OK**.

Sette opp en plan for bleking av ledig plass

MERK: Bleking av ledig plass er aktuelt for aktiva som du sletter ved hjelp av Windows Papirkurv, og for aktiva som slettes manuelt. Bleking av ledig plass gjør ikke makulerte aktiva sikrere.

Slik setter du opp en plan for bleking av ledig plass:

1. Åpne File Sanitizer (filrensing) og klikk på **Free Space Bleaching** (bleking av ledig plass).
2. Merk av for **Activate Scheduler** (aktiv planlegger), skriv inn Windows-passordet og oppgi dag og klokkeslett for bleking av harddisken.
3. Klikk på **Bruk** og deretter på **OK**.

MERK: Bleking av ledig plass kan ta lang tid. Selv om bleking av ledig plass foregår i bakgrunnen, kan datamaskinen bli tregere på grunn av økt bruk av prosessoren.

Velge eller opprette en makuleringsprofil

Du kan angi en slettemetode og velge aktiva som skal makuleres, ved å velge en forhåndsdefinert profil eller opprette en egen profil.

Velge en forhåndsdefinert makuleringsprofil

Hvis du velger en forhåndsdefinert makuleringsprofil (High Security, Medium Security eller Low Security (høy, middels eller lav sikkerhet)), velges en forhåndsdefinert slettemetode og liste over aktiva automatisk. Du kan klikke på **View Details** (vis detaljer) for å vise den forhåndsdefinerte listen over aktiva som er valgt for makulering.

Slik velger du en forhåndsdefinert makuleringsprofil:

1. Åpne File Sanitizer (filrensing) og klikk på **Settings** (innstillinger).
2. Klikk på en forhåndsdefinert makuleringsprofil.
3. Klikk på **View Details** (vis detaljer) for å vise listen over aktiva som er valgt for makulering.
4. Under **Shred the following** (makuler følgende) merker du av ved siden av alle aktiva som du vil bekrefte makulering av.
5. Klikk på **Bruk** og deretter på **OK**.

Lage en egendefinert makuleringsprofil

Når du oppretter en makuleringsprofil, angir du antall makuleringssykluser, hvilke aktiva som skal tas med i makuleringen, hvilke aktiva som skal bekreftes før makulering, og hvilke aktiva som skal utelukkes fra makuleringen:

1. Åpne File Sanitizer (filrensing) og klikk på **Settings** (innstillinger), **Advanced Security Settings** (avanserte sikkerhetsinnstillinger) og deretter på **View Details** (vis detaljer).
2. Angi antall makuleringssykluser.

MERK: Det valgte antall makuleringssykluser utføres for alle aktiva. Hvis du for eksempel velger tre makuleringssykluser, utføres algoritmen som skjuler dataene, tre særskilte ganger. Hvis du velger å bruke et større antall makuleringssykluser, kan makuleringen ta betydelig lengre tid, men jo større antall makuleringssykluser du angir, desto mindre sannsynlig er det at dataene kan gjenskapes.

3. Velg hvilke aktiva som skal makuleres:

   a. Under **Available shred options** (tilgjengelige makuleringsalternativer) klikker du på aktiva og deretter på **Add** (legg til).

   b. Hvis du skal legge til egendefinerte aktiva, klikker du på **Add Custom Option** (legg til egendefinert alternativ) og blar til eller skriver banen til filnavnet eller mappen. Klikk på **Åpne** og deretter på **OK**. Under **Available shred options** (tilgjengelige makuleringsalternativer) klikker du på det egendefinerte alternativet og deretter på **Add** (legg til).

MERK: Hvis du vil fjerne et av de tilgjengelige makuleringsalternativene, klikker du på det og deretter på **Delete** (slett).

4. Under **Shred the following** (makuler følgende) merker du av ved siden av alle aktiva som du vil bekrefte makulering av.

MERK: Hvis du vil fjerne aktiva fra makuleringslisten, klikker du på dem og deretter på **Remove** (fjern).

5. Hvis du vil beskytte filer eller mapper mot automatisk makulering, klikker du på **Add** (legg til) under **Do not shred the following** (ikke makuler følgende) og blar til eller skriver banen til filnavnet eller mappen. Klikk på **Åpne** og deretter på **OK**.

MERK: Hvis du vil fjerne aktiva fra ekskluderingslisten, klikker du på dem og deretter på **Delete** (slett).

6. Når du er ferdig med å sette opp makuleringsprofilen, klikker du på **Bruk** og deretter på **OK**.

Lage en egendefinert profil for enkel sletting

Profilen for enkel sletting utfører vanlig sletting av aktiva uten makulering. Når du lager en egendefinert profil for enkel sletting, angir du hvilke aktiva som skal tas med i slettingen, hvilke aktiva som skal bekreftes før slettingen utføres, og hvilke aktiva som skal utelukkes fra slettingen.

MERK: Hvis du bruker det enkle slettealternativet, kan bleking av ledig plass utføres fra tid til annen på aktiva som er slettet manuelt eller ved hjelp av Windows Papirkurv.

Slik lager du en egendefinert profil for enkel sletting:

1. Åpne File Sanitizer (filrensing) og klikk på **Settings** (innstillinger), **Simple Delete Setting** (innstilling for enkel sletting) og deretter på **View Details** (vis detaljer).

2. Velg hvilke aktiva du vil slette:

   a. Under **Available delete options** (tilgjengelige slettealternativer) klikker du på aktiva og deretter på **Add** (legg til).

   b. Hvis du vil legge til egendefinerte aktiva, klikker du på **Add Custom Option** (legg til egendefinert alternativ), skriver inn et fil- eller mappenavn og klikker på **OK**. Klikk på egendefinerte aktiva og deretter på **Add** (legg til).

MERK: Hvis du vil slette aktiva fra de tilgjengelige slettealternativene, klikker du på dem og deretter på **Delete** (slett).

3. Under **Delete the following** (slett følgende) merker du av alle aktiva som du vil bekrefte slettingen av.

MERK: Hvis du vil fjerne aktiva fra slettelisten, klikker du på aktivaene og deretter på **Remove** (fjern).

4. Under **Do not delete the following** (ikke slett følgende) klikker du på **Add** (legg til) for å velge aktiva som skal utelukkes fra sletting.

MERK: Hvis du vil fjerne aktiva fra ekskluderingslisten, klikker du på dem og deretter på **Delete** (slett).

5. Når du er ferdig med å sette opp profilen for enkel sletting, klikker du på **Bruk** og deretter på **OK**.

Generelle oppgaver

Du kan bruke File Sanitizer (filrensing) til å utføre disse oppgavene:

- Bruke en tastsekvens til å starte makulering – Ved hjelp av denne funksjonen kan du opprette en tastsekvens, for eksempel ctrl+alt+s) for å iverksette makulering. Se Bruke en tastsekvens til å starte makulering på side 74 for å få mer informasjon.
- Bruke File Sanitizer-ikonet til å starte makulering – Denne funksjonen likner dra-og-slipp-funksjonen i Windows. Se Bruke File Sanitizer-ikonet på side 75 for å få mer informasjon.
- Makulere bestemte eller alle valgte aktiva manuelt – Ved hjelp av disse funksjonene kan makulere aktiva manuelt uten å vente på at det gjøres med den regelmessige makuleringsplanen. Se Makulere enkeltaktiva manuelt på side 75 eller Makulere alle valgte elementer manuelt på side 75 for å få mer informasjon.
- Aktivere bleking av ledig plass manuelt – Ved hjelp av denne funksjonen kan du aktivere bleking av ledig plass manuelt. Se Aktivere bleking av ledig plass manuelt på side 76 for å få mer informasjon.
- Avbryte makulering eller bleking av ledig plass – Ved hjelp av denne funksjonen kan du stoppe makulering eller bleking av ledig plass i prosessen. Se Avbryte makulering eller bleking av ledig plass på side 76 for å få mer informasjon.
- Vise loggfilene – Ved hjelp av denne funksjonen kan du vise loggfilene for makulering og bleking av ledig plass, som vil vise eventuelle feil eller mangler i den siste makulerings- eller blekingsprosessen. Se Vise loggfiler på side 76 for å få mer informasjon.

MERK: Makulerings- eller blekingsprosessen kan ta nokså lang tid. Selv om makuleringen eller blekingen av ledig plass skjer i bakgrunnen, kan datamaskinen bli tregere på grunn av den økte bruken av prosessoren.

Bruke en tastsekvens til å starte makulering

Slik angir du en tastsekvens:

1. Åpne File Sanitizer (filrensing) og klikk på **Shred** (makuler).
2. Merk av for **Key sequence** (tastsekvens).
3. Skriv et tegn i tekstboksen.
4. Merk av for enten **CTRL** eller **ALT**, og velg deretter **SHIFT** (skift).

   Hvis du for eksempel vil starte automatisk makulering ved å bruke s-tasten og ctrl+skift, skriver du `s` i tekstboksen og merker av i avkrysningsboksene **CTRL** og **SHIFT** (skift).

   MERK: Pass på at du velger en tastsekvens som er forskjellig fra andre tastsekvenser du har konfigurert.

Slik starter du makulering med en tastsekvens:

1. Hold skift-tasten nede sammen med ctrl- eller alt-tasten (avhengig av hvilken kombinasjon du har angitt) mens du trykker på det valgte tegnet.
2. Hvis en bekreftelsesdialogboks åpnes, klikker du på **Yes** (ja).

Bruke File Sanitizer-ikonet

△ **FORSIKTIG:** Makulerte aktiva kan ikke gjenopprettes. Vurder nøye hvilke elementer du vil velge for manuell makulering.

1. Naviger til dokumentet eller mappen du vil makulere.
2. Dra valgte aktiva til ikonet **File Sanitizer** (filrensing) på skrivebordet.
3. Når bekreftelsesdialogboksen åpnes, klikker du på **Yes** (ja).

Makulere enkeltaktiva manuelt

△ **FORSIKTIG:** Makulerte aktiva kan ikke gjenopprettes. Vurder nøye hvilke elementer du vil velge for manuell makulering.

1. Høyreklikk på **HP ProtectTools**-ikonet i systemstatusfeltet helt til høyre på oppgavelinjen, klikk på **File Sanitizer** (filrensing) og klikk deretter på **Shred One** (enkeltmakulering).
2. Når Bla gjennom-dialogboksen åpnes, navigerer du til aktiva du vil slette, og klikker på **OK**.

MERK: Valgte aktiva kan være en enkelt fil eller mappe.

3. Når bekreftelsesdialogboksen åpnes, klikker du på **Yes** (ja).

– eller –

1. Høyreklikk på **File Sanitizer**-ikonet på skrivebordet og klikk på **Shred One** (enkeltmakulering).
2. Når Bla gjennom-dialogboksen åpnes, navigerer du til aktiva du vil slette, og klikker på **OK**.
3. Når bekreftelsesdialogboksen åpnes, klikker du på **Yes** (ja).

– eller –

1. Åpne File Sanitizer (filrensing) og klikk på **Shred** (makuler).
2. Klikk på **Bla gjennom**.
3. Når Bla gjennom-dialogboksen åpnes, navigerer du til aktiva du vil slette, og klikker på **OK**.
4. Når bekreftelsesdialogboksen åpnes, klikker du på **Yes** (ja).

Makulere alle valgte elementer manuelt

1. Høyreklikk på **HP ProtectTools**-ikonet i systemstatusfeltet helt til høyre på oppgavelinjen, klikk på **File Sanitizer** (filrensing) og klikk deretter på **Shred Now** (makuler nå).
2. Når bekreftelsesdialogboksen åpnes, klikker du på **Yes** (ja).

– eller –

1. Høyreklikk på **File Sanitizer**-ikonet på skrivebordet og klikk deretter på **Shred Now** (makuler nå).
2. Når bekreftelsesdialogboksen åpnes, klikker du på **Yes** (ja).

– eller –

1. Åpne File Sanitizer (filrensing) og klikk på **Shred** (makuler).
2. Klikk på **Shred now** (makuler nå).
3. Når bekreftelsesdialogboksen åpnes, klikker du på **Yes** (ja).

Aktivere bleking av ledig plass manuelt

1. Høyreklikk på **HP ProtectTools**-ikonet i systemstatusfeltet helt til høyre på oppgavelinjen, klikk på **File Sanitizer** (filrensing) og klikk deretter på **Bleach Now** (blek nå).
2. Når bekreftelsesdialogboksen åpnes, klikker du på **Yes** (ja).

– eller –

1. Åpne File Sanitizer (filrensing) og klikk på **Free Space Bleaching** (bleking av ledig plass).
2. Klikk på **Bleach Now** (blek nå).
3. Når bekreftelsesdialogboksen åpnes, klikker du på **Yes** (ja).

Avbryte makulering eller bleking av ledig plass

Det vises en melding over HP ProtectTools Security Manager-ikonet i systemstatusfeltet mens makuleringen eller blekingen av ledig plass pågår. Meldingen inneholder detaljer om makuleringen eller blekingen av ledig plass (prosent fullført) og gir deg mulighet til å avbryte operasjonen.

Slik avbryter du operasjonen:

▲ Klikk på meldingen og deretter på **Stop** (stopp) for å avbryte operasjonen.

Vise loggfiler

Hver gang makulering eller bleking av ledig plass utføres, genereres det loggfiler med eventuelle feil eller mangler. Loggfilene blir alltid oppdatert i forbindelse med den siste makuleringen eller blekingen av ledig plass.

MERK: Filer som er makulert eller bleket riktig, vises ikke i loggfilene.

Det lages én loggfil for makuleringsoperasjoner og en annen loggfil for bleking av ledig plass. Begge loggfilene plasseres i denne katalogen på harddisken:

- C:\Programfiler\Hewlett-Packard\File Sanitizer*[Brukernavn]*_ShredderLog.txt
- C:\Programfiler\Hewlett-Packard\File Sanitizer*[Brukernavn]*_DiskBleachLog.txt

11 Device Access Manager (tilgangsbehandling) for HP ProtectTools (kun på enkelte modeller)

Windows®-operativsystemadministratorer bruker Device Access Manager (tilgangsbehandling) for HP ProtectTools til å styre tilgangen til enheter i et system og beskytte det mot uautorisert tilgang:

- Det opprettes enhetsprofiler for hver bruker for å angi hvilke enheter de har tilgang til eller er nektet tilgang til.
- Brukerne er også ordnet i grupper, for eksempel forhåndsdefinerte grupper av enhetsadministratorer, eller gruppene kan defineres ved hjelp av alternativet Datamaskinbehandling under Administrative verktøy i Kontrollpanel.
- Tilgang til enheter kan gis og nektes på grunnlag av medlemskap i grupper.
- Når det gjelder klasser som CD-ROM- og DVD-stasjoner, kan lesetilgang og skrivetilgang gis og nektes hver for seg.

Brukere med begrensninger kan også gis tillatelse til å lese eller endre tilgangskontrollpolicyen for enheter.

Installeringsprosedyrer

Åpne Device Access Manager (tilgangsbehandling)

Følg denne fremgangsmåten for å åpne Device Access Manager (tilgangsbehandling):

1. Klikk på **Start**, **Alle programmer**, **HP** og deretter på **HP ProtectTools Administrative Console** (administrasjonskonsoll).
2. Klikk på **Device Access Manager** (tilgangsbehandling) i det venstre panelet.

Konfigurere tilgangen til enheter

Device Access Manager (tilgangsbehandling) for HP ProtectTools har tre oversikter:

- Den enkle konfigurasjonsoversikten brukes for å gi eller nekte medlemmer av gruppen enhetsadministratorer tilgang til klasser av enheter.
- Oversikten over enhetsklassekonfigurasjoner brukes for å gi eller nekte bestemte brukere eller gruppen tilgang til typer av enheter eller bestemte enheter.
- Oversikten over brukertilgangsinnstillinger brukes til å angi hvilke brukere som kan vise eller endre enkle konfigurasjoner eller enhetsklassekonfigurasjoner.

Enhetsadministratorgruppen

Når Device Access Manager (tilgangsbehandling) installeres, opprettes en enhetsadministratorgruppe.

Systemadministratoren kan implementere en enkel tilgangskontrollpolicy for enheter ved å nekte tilgang til et sett av enhetsklasser hvis brukeren ikke er klassifisert som klarert (med hensyn til enhetstilgang). Den anbefalte måten å skille mellom "enhetsklarerte" og "ikke enhetsklarerte" brukere på er å gjøre alle "enhetsklarerte" brukere til medlemmer av enhetsadministratorgruppen. Når medlemmer i enhetsadministratorgruppen gis tilgang til enheter via oversikten for enkel konfigurasjon eller konfigurasjon av enhetsklasser, vil dette sørge for at "enhetsklarerte" brukere får full tilgang til det angitte settet med enhetsklasser.

MERK: En bruker får ikke automatisk tilgang til enheter ved å bli innlemmet i enhetsadministratorgruppen. Den enkle konfigurasjonsoversikten kan imidlertid brukes til å gi "enhetsklarerte" brukere tilgang til det nødvendige settet av enhetsklasser.

Følg denne fremgangsmåten for å legge til brukere i enhetsadministratorgruppen:

- Når det gjelder Windows 7, Vista og XP Professional, bruker du MMC-standardmodulen "Lokale brukere og grupper".
- Når det gjelder hjemmeversjoner av Windows 7, Vista® og XP, må du ha administratorrettigheter og skrive følgende i et ledetekstvindu:

```
c:\> net localgroup “Device Administrators” brukernavn /ADD
```

Enkel konfigurasjon

Administratorer og autoriserte brukere kan bruke den enkle konfigurasjonsoversikten til å endre tilgangen til følgende klasser av enheter for alle ikke-enhetsadministratorer.

MERK: For å bruke denne oversikten til å lese informasjon om tilgangen til enheter, må brukeren eller gruppen få "lese"-tilgang i oversikten **User Access Settings** (brukertilgangsinnstillinger). For å bruke denne oversikten til å endre informasjon om tilgangen til enheter, må brukeren eller gruppen få "endre"-tilgang i oversikten **User Access Settings** (brukertilgangsinnstillinger).

- Alle flyttbare medier (disketter, USB-flash-stasjoner, osv.)
- Alle DVD/CD-ROM-stasjoner
- Alle seriell- og parallellporter
- Alle Bluetooth®-enheter
- Alle infrarøde enheter
- Alle modemenheter
- Alle PCMCIA-enheter
- Alle 1394-enheter

Følg denne fremgangsmåten for å gi eller nekte alle ikke-enhetsadministratorer tilgang til en klasse av enheter:

1. I det venstre panelet av **HP ProtectTools Administrative Console** (administrasjonskonsoll) klikker du på **Device Access Manager** (tilgangsbehandling) og deretter på **Simple Configuration** (enkel konfigurasjon).
2. Merk av i avkrysningsboksen til en enhetsklasse eller bestemt enhet i det høyre panelet for å nekte tilgang. Opphev merkingen av den aktuelle enhetsklassen eller bestemte enheten for å gi tilgang.

   Hvis en avkrysningsboks er nedtonet, er verdier som berører tilgangsscenariet blitt endret i konfigurasjonsoversikten for enhetsklasser. Hvis du vil tilbakestille verdiene til enkle innstillinger, klikker du på avmerkingsboksen for å angi eller oppheve den, og klikker deretter på **Yes** (ja) for å bekrefte.
3. Klikk på **Lagre**-ikonet.

   MERK: Hvis bakgrunnstjenesten ikke kjører, åpnes en dialogboks med spørsmål om du vil starte den. Klikk på **Yes** (ja).
4. Klikk på **OK**.

Starte bakgrunnstjenesten

Før enhetsprofiler kan tas i bruk, åpner HP ProtectTools Security Manager en dialogboks med spørsmål om du vil starte bakgrunnstjenesten HP ProtectTools Device Locking/Auditing. Klikk på **Yes** (ja). Bakgrunnstjenesten starter og vil deretter starte automatisk hver gang systemet startes.

MERK: En enhetsprofil må defineres før spørsmålet om bakgrunnstjeneste vises.

Administratorer kan også starte eller stoppe denne tjenesten:

1. Klikk på **Start** og deretter på **Kontrollpanel**.
2. Klikk på **Administrative verktøy** og deretter på **Tjenester**.
3. Søk etter tjenesten **HP ProtectTools Device Locking/Auditing**.

Stopping av Device Locking/Auditing-tjenesten stopper ikke enhetslåsing. To komponenter sørger for enhetslåsing:

- Device Locking/Auditing-tjenesten
- DAMDrv.sys-driveren

Starting av tjenesten starter enhetsdriveren, men stopping av tjenesten stopper ikke driveren.

Hvis du vil finne ut om bakgrunnstjenesten kjører, åpner du et ledetekstvindu og skriver sc query flcdlock.

Hvis du vil finne ut om enhetsdriveren kjører, åpner du et ledetekstvindu og skriver sc query damdrv.

Enhetsklassekonfigurasjon

Administratorer og autoriserte brukere kan vise og endre lister over brukere og grupper som gis eller nektes tilgang til klasser av enheter eller bestemte enheter.

MERK: For å bruke denne oversikten til å lese informasjon om tilgangen til enheter, må brukeren eller gruppen få "lese"-tilgang i oversikten **User Access Settings** (brukertilgangsinnstillinger). For å bruke denne oversikten til å endre informasjon om tilgangen til enheter, må brukeren eller gruppen få "endre"-tilgang i oversikten **User Access Settings** (brukertilgangsinnstillinger).

Oversikten Device Class Configuration (konfigurasjon av enhetsklasser) består av disse delene:

- **Device List** (enhetsliste) – Viser alle enhetsklasser og enheter som er installert på systemet eller som kan ha vært installert på systemet tidligere.
  - Beskyttelse angis vanligvis for hele enhetsklasser. En valgt bruker eller gruppe vil få tilgang til alle enheter i enhetsklassen.
  - Beskyttelse kan også angis for bestemte enheter.
- **User List** (brukerliste) – Viser alle brukere og grupper som gis eller nektes tilgang til den valgte enhetsklassen eller bestemte enheten.
  - Brukerlisteoppføringer kan gjelde bestemte brukere eller gruppen som brukerne er medlem av.
  - Hvis en bruker- eller gruppeoppføring i brukerlisten er utilgjengelig, er innstillingen arvet fra enhetsklassen i enhetslisten eller fra klassemappen.
  - Enkelte enhetsklasser, som DVD og CD-ROM, kan spesifiseres nærmere ved å gi eller nekte tilgang til lese- og skriveoperasjoner særskilt.

    Når det gjelder andre enheter og klasser, kan lese- og skrivetilgangsrettigheter arves. Lesetilgang kan for eksempel arves fra en overordnet klasse, mens skrivetilgang kan nektes en bruker eller gruppe særskilt.

    MERK: Hvis avkrysningsboksen for lesetilgang står åpen, har ikke tilgangskontrolloppføringen noen betydning for lesetilgangen til enheten. Den verken gir eller nekter lesetilgang til enheten.

    Eksempel 1 – Hvis en bruker eller gruppe nektes skrivetilgang til en enhet eller klasse av enheter:

    Samme bruker, samme gruppe eller et medlem av samme gruppe kan bare gis skrivetilgang eller lese- og skrivetilgang til enheter under denne enheten i enhetshierarkiet.

Eksempel 2 – Hvis en bruker eller gruppe gis skrivetilgang til en enhet eller klasse av enheter:

Samme bruker, samme gruppe eller et medlem av samme gruppe kan bare nektes skrivetilgang eller lese- og skrivetilgang til samme enhet eller enheter under denne enheten i enhetshierarkiet.

Eksempel 3 – Hvis en bruker eller gruppe gis lesetilgang til en enhet eller klasse av enheter:

Samme bruker, samme gruppe eller et medlem av samme gruppe kan bare nektes lesetilgang eller lese- og skrivetilgang til samme enhet eller enheter under denne enheten i enhetshierarkiet.

Eksempel 4 – Hvis en bruker eller gruppe nektes lesetilgang til en enhet eller klasse av enheter:

Samme bruker, samme gruppe eller et medlem av samme gruppe kan bare gis lesetilgang eller lese- og skrivetilgang til enheter under denne enheten i enhetshierarkiet.

Eksempel 5 – Hvis en bruker eller gruppe gis lese- og skrivetilgang til en enhet eller klasse av enheter:

Samme bruker, samme gruppe eller et medlem av samme gruppe kan bare nektes skrivetilgang eller lese- og skrivetilgang til samme enhet eller enheter under denne enheten i enhetshierarkiet.

Eksempel 6 – Hvis en bruker eller gruppe nektes lese- og skrivetilgang til en enhet eller klasse av enheter:

Samme bruker, samme gruppe eller et medlem av samme gruppe kan bare gis lesetilgang eller lese- og skrivetilgang til enheter under denne enheten i enhetshierarkiet.

Nekte en bruker eller gruppe tilgang

Følg denne fremgangsmåten for å hindre at en bruker eller gruppe får tilgang til en enhet eller klasse av enheter:

1. I det venstre panelet av **HP ProtectTools Administrative Console** (administrasjonskonsoll) klikker du på **Device Access Manager** (tilgangsbehandling) og deretter på **Device Class Configuration** (konfigurasjon av enhetsklasser).
2. Klikk på enhetsklassen du vil konfigurere, i enhetslisten.
   - Enhetsklasse
   - Alle enheter
   - Enkeltenhet
3. Under **User/Groups** (brukere/grupper) klikker du på brukeren eller gruppen som skal nektes tilgang.
4. klikk på **Deny** (nekt) ved siden av en bruker eller gruppe.
5. Klikk på **Lagre**-ikonet.

MERK: Hvis innstillinger for å nekte og gi tilgang angis på samme enhetsnivå for en bruker, vil nektingen av tilgang overstyre den andre innstillingen.

Gi en bruker eller gruppe tilgang

Følg denne fremgangsmåten for å gi en bruker eller gruppe tilgang til en enhet eller klasse av enheter:

1. I det venstre panelet av **HP ProtectTools Administrative Console** (administrasjonskonsoll) klikker du på **Device Access Manager** (tilgangsbehandling) og deretter på **Device Class Configuration** (konfigurasjon av enhetsklasser).
2. Klikk på ett av følgende i enhetslisten:
   - Enhetsklasse
   - Alle enheter
   - Enkeltenhet
3. Klikk på **Add** (legg til).

   Dialogboksen **Select Users or Groups** (velg brukere eller grupper) åpnes.
4. Klikk på **Advanced** (avansert) og deretter på **Find Now** (finn nå) for å søke etter brukere eller grupper som skal legges til.
5. Klikk på en bruker eller gruppe som skal legges til listen over tilgjengelige brukere og grupper, og klikk på **OK**.
6. Klikk på **OK** en gang til.
7. Klikk **Allow** (tillat) for å gi denne brukeren eller gruppen tilgang.
8. Klikk på **Lagre**-ikonet.

Fjerne en bruker eller gruppes tilgang

Følg denne fremgangsmåten for å fjerne en bruker eller gruppes tilgang til en enhet eller klasse av enheter:

1. I det venstre panelet av **HP ProtectTools Administrative Console** (administrasjonskonsoll) klikker du på **Device Access Manager** (tilgangsbehandling) og deretter på **Device Class Configuration** (konfigurasjon av enhetsklasser).
2. Klikk på enhetsklassen du vil konfigurere, i enhetslisten.
   - Enhetsklasse
   - Alle enheter
   - Enkeltenhet
3. Under **User/Groups** (brukere/grupper) klikker du på brukeren eller gruppen du vil fjerne, og deretter på **Remove** (fjern).
4. Klikk på **Lagre**-ikonet.

Gi én bruker i en gruppe tilgang til en klasse av enheter

Følg denne fremgangsmåten for å gi en bruker tilgang til en klasse av enheter samtidig som alle andre medlemmer i brukerens gruppe nektes tilgang:

1. I det venstre panelet av **HP ProtectTools Administrative Console** (administrasjonskonsoll) klikker du på **Device Access Manager** (tilgangsbehandling) og deretter på **Device Class Configuration** (konfigurasjon av enhetsklasser).
2. Klikk på enhetsklassen du vil konfigurere, i enhetslisten.
   - Enhetsklasse
   - Alle enheter
   - Enkeltenhet
3. Under **User/Groups** (brukere/grupper) velger du gruppen som skal nektes tilgang, og klikker på **Deny** (nekt).
4. Naviger til mappen under den aktuelle klassen, og legg deretter inn den bestemte brukeren.
5. Klikk på **Allow** (tillat) for å gi denne brukeren tilgang.
6. Klikk på **Lagre**-ikonet.

Gi én bruker i en gruppe tilgang til en bestemt enhet

Administratorer kan gi en bruker tilgang til en bestemt enhet samtidig som alle andre medlemmer av brukerens gruppe nektes tilgang til alle enheter i klassen:

1. I det venstre panelet av **HP ProtectTools Administrative Console** (administrasjonskonsoll) klikker du på **Device Access Manager** (tilgangsbehandling) og deretter på **Device Class Configuration** (konfigurasjon av enhetsklasser).
2. Klikk på enhetsklassen du vil konfigurere, i enhetslisten, og naviger deretter til mappen under denne.
3. Klikk på **Add** (legg til). Dialogboksen **Select Users or Groups** (velg brukere eller grupper) åpnes.
4. Klikk på **Advanced** (avansert) og deretter på **Find Now** (finn nå) for å søke etter brukergruppen som skal nektes tilgang til alle enheter i klassen.
5. Klikk på gruppen og deretter på **OK**.
6. Naviger til den bestemte enheten under enhetsklassen, som brukeren skal gis tilgang til.
7. Klikk på **Add** (legg til). Dialogboksen **Select Users or Groups** (velg brukere eller grupper) åpnes.
8. Klikk på **Advanced** (avansert) og deretter på **Find Now** (finn nå) for å søke etter brukere eller grupper som skal legges til.
9. Klikk på brukeren som skal gis tilgang, og deretter på **OK**.
10. Klikk på **Allow** (tillat) for å gi denne brukeren tilgang.
11. Klikk på **Lagre**-ikonet.

Tilbakestille konfigurasjonen

△ **FORSIKTIG:** Tilbakestilling av konfigurasjonen forkaster alle endringer i enhetskonfigurasjoner som er gjort, og setter alle innstillinger tilbake til verdiene som var angitt fra fabrikk.

Følg denne fremgangsmåten for å tilbakestille konfigurasjonsinnstillingene til fabrikkverdiene:

1. I det venstre panelet av **HP ProtectTools Administrative Console** (administrasjonskonsoll) klikker du på **Device Access Manager** (tilgangsbehandling) og deretter på **Device Class Configuration** (konfigurasjon av enhetsklasser).
2. Klikk på **Reset** (tilbakestill).
3. Klikk på **Yes** (ja) for å bekrefte.
4. Klikk på **Lagre**-ikonet.

Avanserte oppgaver

Styre tilgangen til konfigurasjonsinnstillingene

I oversikten **User Access Settings** (brukertilgangsinnstillinger) kan administratorer angi hvilke brukere eller grupper som har tilgang til sidene Simple Configuration (enkel konfigurasjon) og Device Class Configuration (konfigurasjon av enhetsklasser).

MERK: En bruker eller gruppe må ha "fulle brukeradministratorrettigheter" for å kunne endre innstillingene i oversikten User Access Settings (brukertilgangsinnstillinger).

- En bruker eller gruppe må gis tilgangen "View (Read-only) Configuration Settings" (vis konfigurasjonsinnstillinger) i oversikten User Access Settings (brukertilgangsinnstillinger) for å vise informasjon på oversiktene for enkel konfigurasjon og konfigurasjon av enhetsklasser.
- En bruker eller gruppe må gis tilgangen "Change Configuration Settings" (endre konfigurasjonsinnstillinger) i oversikten User Access Settings (brukertilgangsinnstillinger) for å endre informasjon på oversiktene for enkel konfigurasjon og konfigurasjon av enhetsklasser.

MERK: Selv medlemmer av administratorgruppen må få "lese"-tilgang for å kunne vise oversiktene for enkel konfigurasjon og konfigurasjon av enhetsklasser og "endre"-tilgang for å kunne endre data på oversiktene for enkel konfigurasjon og konfigurasjon av enhetsklasser.

MERK: Hvis en bruker etter kontroll av tilgangsnivåene til alle brukere og grupper verken har tilgang eller er nektet tilgang til et bestemt tilgangsnivå, blir brukeren nektet tilgang på det nivået.

Gi en eksisterende gruppe eller bruker tilgang

Følg denne fremgangsmåten for å gi en eksisterende gruppe eller bruker tillatelse til å vise eller endre konfigurasjonsinnstillingene:

1. I det venstre panelet av **HP ProtectTools Administrative Console** (administrasjonskonsoll) klikker du på **Device Access Manager** (tilgangsbehandling) og deretter på **User Access Settings** (brukertilgangsinnstillinger).
2. Klikk på en gruppe eller brukes som skal gis tilgang.
3. Under **Permissions** (tillatelser) klikker du på **Allow** (tillat) for alle typer tillatelse den valgte gruppen eller brukeren skal få:

   MERK: Tillatelsene som gis er kumulative. En bruker som gis tillatelsen "Change Configuration Settings" (endre konfigurasjonsinnstillinger), får automatisk tillatelsen "View (Read-only) Configuration Settings" (vis konfigurasjonsinnstillinger). En bruker som gis "Full User Administrator Rights" (fulle brukeradministratorrettigheter), får også tillatelsene "Change Configuration Settings" og "View (Read-only) Configuration Settings".

   - Fulle brukeradministratorrettigheter
   - Endre konfigurasjonsinnstillinger
   - Vis konfigurasjonsinnstillinger
4. Klikk på **Lagre**-ikonet.

Nekte en eksisterende gruppe eller bruker tilgang

Følg denne fremgangsmåten for å nekte en eksisterende gruppe eller bruker tillatelse til å vise eller endre konfigurasjonsinnstillingene:

1. I det venstre panelet av **HP ProtectTools Administrative Console** (administrasjonskonsoll) klikker du på **Device Access Manager** (tilgangsbehandling) og deretter på **User Access Settings** (brukertilgangsinnstillinger).
2. Klikk på en gruppe eller brukes som skal nektes tilgang.
3. Under **Permissions** (tillatelser) klikker du på **Deny** (nekt) for alle typer tillatelse den valgte gruppen eller brukeren skal nektes:
   - Fulle brukeradministratorrettigheter
   - Endre konfigurasjonsinnstillinger
   - Vis konfigurasjonsinnstillinger
4. Klikk på **Lagre**-ikonet.

Legge til en ny gruppe eller bruker

Følg denne fremgangsmåten for å gi en ny gruppe eller bruker tillatelse til å vise eller endre konfigurasjonsinnstillingene:

1. I det venstre panelet av **HP ProtectTools Administrative Console** (administrasjonskonsoll) klikker du på **Device Access Manager** (tilgangsbehandling) og deretter på **User Access Settings** (brukertilgangsinnstillinger).
2. Klikk på **Add** (legg til). Dialogboksen **Select Users or Groups** (velg brukere eller grupper) åpnes.
3. Klikk på **Advanced** (avansert) og deretter på **Find Now** (finn nå) for å søke etter brukere eller grupper som skal legges til.
4. Klikk på en gruppe eller bruker, klikk på **OK** og deretter på **OK** igjen.
5. Klikk på **Allow** (tillat) for å gi denne brukeren tilgang.
6. Klikk på **Lagre**-ikonet.

Fjerne en gruppe eller brukers tilgang

Følg denne fremgangsmåten for å fjerne en gruppe eller brukers tillatelse til å vise eller endre konfigurasjonsinnstillingene:

1. I det venstre panelet av **HP ProtectTools Administrative Console** (administrasjonskonsoll) klikker du på **Device Access Manager** (tilgangsbehandling) og deretter på **User Access Settings** (brukertilgangsinnstillinger).
2. Klikk på en gruppe eller bruker, og klikk deretter på **Remove** (fjern).
3. Klikk på **Lagre**-ikonet.

Beslektet dokumentasjon

Device Access Manager (tilgangsbehandling) for HP ProtectTools er kompatibel med foretaksproduktet HP ProtectTools Enterprise Device Access Manager. Ved bruk sammen med foretaksproduktet gir Device Access Manager (tilgangsbehandling) for HP ProtectTools bare lesetilgang til egne funksjoner.

Mer informasjon om Device Access Manager (tilgangsbehandling) for HP ProtectTools er tilgjengelig på nettadressen http://www.hp.com/hps/security/products.

12 LoJack Pro for HP ProtectTools

Absolute Softwares serie av Computrace-produkter gjør det mulig for brukere å spore sine HP-datamaskiner og få bedre databeskyttelse. Computrace LoJack-produkter reduserer også tapet av maskiner og bidrar til gjenfinning av stjålne maskiner.

Følg denne veiledningen for å aktivere Computrace-produktet:

1. Klikk på **Start** og **Alle programmer** og deretter på **HP ProtectTools Security Manager**.
2. Klikk på **Theft Recovery** (tyverisikring) og deretter på **Activate Now** (aktiver nå).

   Standardnettleseren åpner en abonnementsnettside hvor du kan velge og kjøpe ett av de tre Computrace-produktene som er tilgjengelig for HP ProtectTools:

   - **Computrace Data Delete** (datasletting) – Inkluderer fjerndatasletting, låsing av enhet og grunnleggende sporing og rapportering av aktiva.
   - **Computrace LoJack Pro** – Inkluderer fjerndatasletting, låsing av enhet, grunnleggende sporing og rapportering av aktiva og styrt tyverisikring.
   - **Computrace LoJack Pro Premium** – Inkluderer fjerndatasletting, låsing av enhet, avansert sporing og rapportering av aktiva, geolokalisering og -inngjerding og styrt tyverisikring.

Computrace-agenten er innebygd i BIOS på HPs bærbare kontordatamaskiner, selv om agenten er slått av ved levering av datamaskinen. Når ddu har kjøpt et abonnement, kan agenten aktiveres. Den innebygde agenten kan installere operativsystemet på nytt og omformatere harddiskene.

MERK: Abonnementsperioder fra 1 til 5 år er tilgjengelig. Se abonnementsavtalen for Absolute Software for å få mer informasjon om dette. Tyverisikringstjenesten er avhengig av den geografiske plasseringen. GPS-sporing støttes på enkelte modeller med WWAN-tilleggsutstyr.

13 Feilsøking

HP ProtectTools Security Manager

Kort beskrivelse	Detaljer	Løsning
Smartkort og USB-token er ikke tilgjengelig i Security Manager (sikkerhetsbehandling) hvis de er installert etter at Security Manager ble installert.	For å kunne bruke smartkort eller USB-token i Security Manager (sikkerhetsbehandling) må støtteprogramvaren (drivere, PKCS#11-leverandører, osv.) være installert før installering av Security Manager. Hvis du allerede har installert Security Manager (sikkerhetsbehandling), må du utføre følgende etter å ha installert støtteprogramvare for smartkort eller token:	Logg deg på Password Manager (passordbehandling). I HP ProtectTools Security Manager klikker du på **Password Manager** (passordbehandling), **Credentials** (påloggingsinformasjon) og deretter **Smart Card** (smartkort). Start datamaskinen på nytt hvis du blir bedt om det.
Noen nettsider i programmer hindrer brukeren i å utføre eller fullføre oppgaver.	Noen webbaserte programmer slutter å fungere og rapporterer feil på grunn av det deaktiverende funksjonalitetsmønsteret i Single Sign On (engangspålogging). I Internet Explorer vil for eksempel et **!** (utropstegn) i en gul trekant angi at det har oppstått en feil.	Security Manager Single Sign On (engangspålogging) støtter ikke webgrensesnittene til all programvare. Deaktiver støtten for engangspålogging for den aktuelle nettsiden ved å slå denne støtten av. Se den fullstendige dokumentasjonen om engangspålogging som er tilgjengelig i hjelpefilene til Security Manager-programvaren. Hvis en bestemt Single Sign On (engangspålogging) ikke kan deaktiveres for et bestemt program, kan du ringe HPs tekniske støtte og be om tredjenivås støtte gjennom din HP-servicekontakt.
Alternativet **Browse for Virtual Token** (søk etter virtuelt token) vises ikke under påloggingsprosessen.	Brukeren kan ikke flytte et registrert virtuelt token i Password Manager (passordbehandling) fordi navigeringsalternativet er fjernet for å redusere sikkerhetsrisikoen.	Muligheten til å søke ble fjernet fordi det tillot at ikke-brukere kunne slette og endre navn på filer, og ta kontroll over Windows.
Domeneadministratorer kan ikke endre Windows-passord selv om de er autoriserte.	Dette skjer når en domeneadministrator logger seg på et domene og registrerer sin domeneidentitet i Password Manager (passordbehandling) ved hjelp av en konto med administratorrettigheter i domenet og på den lokale datamaskinen. Når domeneadministratoren forsøker å endre Windows-passordet i Password Manager (passordbehandling), får hun eller han en påloggingsfeilmelding: **User account restriction** (begrenset brukerkonto).	Password Manager (passordbehandling) kan ikke endre en domenebrukers kontopassord via **Change Windows password** (endre Windows-passord). Security Manager (sikekrhetsbehandling) kan bare endre kontopassord for lokale datamaskiner. Domenebrukere kan endre sitt passord via alternativet **Change password** (endre passord) under **Windows security** (Windows-sikkerhet), men i og med at en domenebruker ikke har noen fysisk konto på den lokale datamaskinen, kan Password Manager (passordbehandling) bare endre passordet som brukes til pålogging.

Kort beskrivelse	Detaljer	Løsning
Password Manager (passordbehandling) har kompatibilitetsproblemer med Corel WordPerfect 12-passordet GINA.	Hvis brukeren logger seg på Password Manager, lager et dokument i WordPerfect og lagrer det med passordbeskyttelse, vil ikke Password Manager kunne gjenkjenne eller oppdage passordet GINA verken manuelt eller automatisk.	HP arbeider for å finne en løsning for fremtidige produktforbedringer.
Password Manager (passordbehandling) gjenkjenner ikke knappen **Connect** (koble til) på skjermen.	Hvis Engangspålogging-legitimasjonen for Tilkobling til eksternt skrivebord er satt til **Koble til**, vises alltid **Lagre som** i stedet for **Koble til** når Engangspålogging startes på nytt.	HP arbeider for å finne en løsning for fremtidige produktforbedringer.
Brukeren får ikke logget seg på Password Manager (passordbehandling) etter en overgang fra vente- til dvalemodus (gjelder bare Windows XP Service Pack 1).	Etter å ha latt systemet gå over i dvale- og hvilemodus får ikke administratoren eller brukeren logget seg på Password Manager og Windows-påloggingsbildet blir stående uansett hvilken påloggingsinformasjon som brukes, enten det er passord, fingeravtrykk eller Java-kort.	Oppdatere Windows til Service Pack 2 via Windows Update. Se Microsofts kunnskapsbaseartikkel 813301 på http://www.microsoft.com hvis du vil ha mer informasjon om årsaken til problemet. For å få logget seg på må brukeren velge Password Manager. Etter å ha logget seg på Password Manager blir brukeren bedt om å logge seg på Windows (brukeren må kanskje velge Windows-påloggingsalternativet) for å fullføre påloggingsprosessen. Hvis brukeren logger seg på Windows først, må hun eller han logge seg på Password Manager manuelt.
Sikkerhetsprosessen **Restore Identity** (gjenopprett identitet) mister tilknytningen til virtuelt token.	Når brukeren gjenoppretter identiteten, kan Password Manager miste kontrollen med hvor det virtuelle tokenet er plassert på påloggingsskjermbildet. Selv om Password Manager har registrert det virtuelle tokenett, må brukeren registrere tokenet på nytt for å gjenopprette forbindelsen.	Dette er for øyeblikket tiltenkt virkemåte. Ved avinstallering av Security Manager uten å beholde identiteter vil serverdelen av systemet bli ødelagt, slik at tokenet ikke lenger kan brukes til pålogging, selv om klientdelen av tokenet gjenopprettes med identitetsgjenoppretting. HP arbeider for å finne langsiktige løsninger.

Device Access Manager (tilgangsbehandling) for HP ProtectTools

Brukere er blitt nektet tilgang til enheter i Device Access Manager (tilgangsbehandling), men enhetene er fremdeles tilgjengelige.

- **Forklaring** – Simple Configuration (enkel konfigurasjon) og/eller Device Class Configuration (konfigurasjon av enhetsklasser) er blitt brukt i Device Access Manager til å nekte brukere tilgang til enheter. På tross av at de er nektet tilgang, får brukerne fremdeles tilgang til enhetene.
- **Løsning:**
  - Kontroller at HP ProtectTools Device Locking-tjenesten er startet.
  - Som administrativ bruker klikker du på **Kontrollpanel** og deretter på **System og vedlikehold**. I vinduet Administrative verktøy klikker du på **Tjenester** og søker etter tjenesten **HP ProtectTools Device Locking/Auditing**. Sørg for at tjenesten er startet og at oppstartstypen er **Automatisk**.

En bruker har uventet tilgang til en enhet, eller en bruker er uventet nektet tilgang til en enhet.

- **Forklaring** – Device Access Manager (tilgangsbehandling) er brukt til å nekte brukere tilgang til enkelte enheter og gi brukere tilgang til andre enheter. Når brukere bruker systemet, får de tilgang til enheter som de tror de er nektet tilgang til i Device Access Manager, og blir nektet tilgang til enheter som de tror Device Access Manager skulle gi tilgang til.
- **Løsning:**
  - Bruk Device Class Configuration (konfigurasjon av enhetsklasser) i Device Access Manager til å undersøke brukeres enhetsinnstilllinger.
  - Klikk på **Security Manager** (sikkerhetsbehandling), **Device Access Manager** (tilgangsbehandling) og deretter på **Device Class Configuration** (konfigurasjon av enhetsklasser). Utvid nivåene på enhetsklassetreet og gå gjennom innstillingene til den aktuelle brukeren. Se etter eventuelle "Deny"-nektelser som kan være angitt for brukeren eller eventuelle Windows-grupper som brukeren er medlem av, for eksempel Brukere eller Administratorer.

Tillatelser eller nektelser, hva har forrang?

- **Forklaring** – I Device Class Configuration (konfigurasjon av enhetsklasser) er følgende konfigurasjon angitt:
  - En Windows-gruppe (f.eks. BUILTIN\Administratorer) har fått tillatelse og en annen Windows-gruppe (f.eks. BUILTIN\Brukere) er nektet tillatelse på samme nivå i hierarkiet av enhetsklasser (f.eks. DVD/CD-ROM-stasjoner).
  - Hvis en bruker er medlem av begge gruppene (f.eks. Administrator), hvilken har forrang?
- **Løsning:**
  - Brukeren blir nektet tilgang til enheten. Nektelser har forrang fremfor tillatelser.
  - Tilgang nektes på grunn av måten Windows kommer frem til den effektive tillatelsen for enheten på. En gruppe nektes og en gruppe tillates, men brukeren er medlem av begge gruppene. Brukeren nektes fordi nektelsen gis forrang fremfor tillatelsen.

- En løsning kan være å nekte gruppen Brukere på nivået DVD/CD-ROM-stasjoner og tillate gruppen Administratorer på nivået under DVD/CD-ROM-stasjoner.
- En annen løsning er å opprette spesielle Windows-grupper, en for å gi tilgang til DVD/CD og en annen for å nekte tilgang til DVD/CD. Da kan hver bruker plasseres i riktig gruppe.

Oversikten Simple Configuration (enkel konfigurasjon) er brukt til å angi en tilgangskontrollpolicy for enheter, men administrative brukere får ikke tilgang til enheter.

- **Forklaring** – Simple Configuration nekter brukere og gjester tilgang, men gir enhetsadministratorer tilgang.
- **Løsning:** Legg den administrative brukeren til gruppen av enhetsadministratorer.

Diverse

Programvarepåvirket – kort beskrivelse	Detaljer	Løsning
Security Manager – mottatt feilmelding: **The security application can not be installed until the HP Protect Tools Security Manager is installed** (sikkerhetsprogrammet kan ikke installeres før HP Protect Tools Security Manager er installert).	Alle sikkerhetsprogrammer som Java Card Security og biometri er utvidbare tilleggsmoduler til Security Manager-grensesnittet. Security Manager (sikkerhetsbehandling) må installeres før en HP-godkjent sikkerhetsmodul kan lastes inn.	Security Manager-programvaren må være installert før eventuelle sikkerhetspluginer installeres.
HP ProtectTools Security Manager – Det oppstår en forbigående feil når grensesnittet for Security Manager lukkes.	Det oppstår en forbigående feil (1 av 12 ganger) når du bruker lukkeknappen øverst til høyre for å lukke Security Manager før alle plugin-programmene er ferdig innlastet.	Dette er relatert til en tidsberegningsavhengighet ved lastetid for plugin-tjenester ved lukking og ny start av Security Manager. Fordi PTHOST.exe er skallet som inneholder de andre programmene (plugin-moduler), er det avhengig av plugin-modulens evne til å fullføre lastetiden (tjenester). Den underliggende årsaken er lukking av skallet før plugin-modulen hadde tid til å bli ferdiglastet. La Security Manager fullføre meldingen om lasting av tjenester (øverst i Security Manager-vinduet) og alle plugin-modulene i venstre kolonne. For å unngå feil må du gi lastingen av disse plugin-modulene litt tid.
HP ProtectTools – Ubegrenset tilgang eller ukontrollerte administratorrettigheter utgjør en sikkerhetsrisiko.	Det er flere farer knyttet til ubegrenset tilgang til datamaskinen, blant annet følgende: • Sletting av PSD • Skadelig endring av brukerinnstillinger • Deaktivering av sikkerhetspolicyer og funsjoner	Administratorer anbefales å følge "anbefalt praksis" når det gjelder begrensning av brukerrettigheter og brukertilgang. Uautoriserte brukere bør ikke innvilges administrative rettigheter.

Ordliste

administrator *Se* Windows-administrator.

aktiva Datakomponenter som består av personlige opplysninger eller filer, historiske eller webrelaterte data og så videre, som er plassert på harddisken.

aktivering Handling som må utføres før noen av funksjonene til Drive Encryption (stasjonskryptering) blir tilgjengelig. Drive Encryption aktiveres ved hjelp av HP ProtectTools Setup Wizard (installasjonsveiviser). Bare administratorer kan aktivere Drive Encryption. Aktiveringsprosessen innbefatter aktivering av programvaren, kryptering av stasjonen, oppretting av en brukerkonto og oppretting av en krypteringsnøkkel for den første sikkerhetskopien på en flyttbar lagringsenhet.

ATM Automatic Technology Manager, som gjør det mulig for nettverksadministratorer å fjernstyre systemer på BIOS-nivå.

automatisk makulering Planlagt makulering som brukeren angir i File Sanitizer (filrensing).

autorisert bruker En bruker som har fått tillatelse via oversikten User Access Settings (brukertilgangsinnstillinger) til å vise eller endre konfigurasjonsinnstillinger i oversiktene Simple Configuration (enkel konfigurasjon) og Device Class Configuration (konfigurasjon av enhetsklasser).

avsløre En handling som gjør brukeren i stand til å dekryptere en eller flere chattelogger og vise kontakters skjermnavn som vanlig tekst og gjøre økten tilgjengelig for visning.

bakgrunnstjeneste HP ProtectTools Device Locking/Auditing-bakgrunnstjenesten, som må være startet for at tilgangskontrollpolicyer for enheter skal tre i kraft. Den kan vises i Tjenester-programmet under alternativet Administrative verktøy i Kontrollpanel. Hvis den ikke er startet, forsøker HP ProtectTools Security Manager å starte den når tilgangskontrollpolicyer for enheter tas i bruk.

biometrisk En type godkjenningsinformasjon som bruker fysiske egenskaper, for eksempel et fingermerke, til å identifisere en bruker.

bleking av ledig plass Sikker skriving av vilkårlige data over slettede aktiva for å forvrenge innholdet i de slettede aktivaene.

bruker Hvem som helst som er registrert i Drive Encryption (stasjonskryptering). Brukere som ikke er administratorer, har begrensede rettigheter i Drive Encryption. De kan registrere seg (med administrators godkjenning) og logge seg på.

chatteloggøkt En kryptert fil som inneholder en logg over begge sider av en samtale i en chatteøkt.

dekryptering Metode innen kryptografi som brukes til å konvertere krypterte data til vanlig tekst.

digital signatur Data som sendes med en fil og som bekrefter avsenderen av materialet, og at filen ikke er blitt endret etter at den ble signert.

digitalt sertifikat Elektronisk legitimasjon som bekrefter identiteten til en enkeltperson eller et selskap ved å knytte identiteten til eieren av det digitale sertifikatet til et par elektroniske nøkler som brukes til å signere digital informasjon.

domene En gruppe av datamaskiner som inngår i et nettverk og som deler en felles katalogdatabase. Domener har unike navn, og de har alle et sett av felles regler og prosedyrer.

Drive Encryption (stasjonskryptering) Beskytter data ved å kryptere harddisker, slik at data blir uleselige for alle uten riktig autorisasjon.

Drive Encryption-påloggingsbilde En påloggingsskjermbilde som vises før Windows startes. Brukere må enten oppgi sitt Windows-brukernavn og -passord eller PIN-koden til Java-kortet. I de fleste tilfeller vil du ved å gi riktige opplysninger på påloggingsbildet for Drive Encryption (stasjonskryptering) få direkte tilgang til Windows uten å måtte logge på igjen på Windows-skjermbildet.

DriveLock Sikkerhetsfunksjon som knytter harddisken til en bruker og krever at brukeren oppgir riktig DriveLock-passord når datamaskinen starter opp.

EFS (Encryption File System) System som krypterer alle filer og undermapper i den valgte mappen.

enhetsklasse Alle enheter av en bestemt type, som stasjoner.

enkel sletting Sletting av Windows-referansen til aktiva. Innholdet i aktiva blir værende på harddisken til dataene tilsløres ved overskriving, såkalt "bleking" av ledig plass.

fingeravtrykk Et digitalt utsnitt av ditt fingeravtrykk. Det faktiske fingeravtrykkbildet blir aldri lagret i Security Manager (sikkerhetsbehandling).

foreslått undertegner En bruker som er utpekt av eieren av et Microsoft Word- eller Microsoft Excel-dokument til å legge til en signaturlinje i dokumentet.

forsegle for klarerte kontakter En handling som innebærer å legge til en digital signatur, kryptere e-post og sende denne etter at du har godkjent deg med en valgt sikkerhetspåloggingsmetode.

gjenopprette En prosess som kopierer programinformasjon fra en tidligere lagret sikkerhetskopifil til dette programmet.

godkjenning Prosess som bekrefter om en bruker er autorisert til å utføre en oppgave, som å få tilgang til en datamaskin, endre innstillinger for et bestemt program eller vise sikre data.

godkjenning før oppstart Sikkerhetsfunksjon som krever en form for godkjenning, for eksempel et Java-kort, en sikkerhetsbrikke eller et passord, når datamaskinen slås på.

gruppe En gruppe brukere med samme nivå av tillatelser eller nektelser for en enhetsklasse eller bestemt enhet.

HP SpareKey (reservenøkkel) Sikkerhetskopi av stasjonskrypteringsnøkkel.

identitet I HP ProtectTools Security Manager er det en gruppe av påloggingsinformasjon og innstillinger som behandles som kontoen eller profilen til en bestemt bruker.

ID-kort Et verktøy på windows-sidepanelet som fungerer som visuell identifikasjon på skrivebordet med brukernavn og et valgt bilde. Klikk på ID-kortet for å åpne HP ProtectTools Administrative Console (administrasjonskonsoll).

instrumentbord En sentral plassering hvor du får tilgang til og kan administrere funksjoner og innstillinger i HP ProtectTools Security Manager (sikkerhetsbehandling).

Java-kort Et flyttbart kort som settes inn i datamaskinen. Det inneholder identifikasjonsopplysninger for pålogging. Pålogging med et Java-kort på påloggingsbildet for Drive Encryption (stasjonskryptering) krever at du setter inn Java-kortet og skriver brukernavnet ditt og PIN-koden til Java-kortet.

katastrofegjenopprettingsarkiv Beskyttet lagringsområde som tillater ny kryptering av BUK-nøkler (Basic User Key) fra én plattformseiernøkkel til en annen.

klarert avsender En klarert kontakt som sender signerte og/eller krypterte e-postmeldinger og Microsoft Office-dokumenter.

klarert IM-kommunikasjon En kommunikasjonsøkt der klarerte meldinger sendes fra en klarert avsender til en klarert kontakt.

klarert kontakt En person som har tatt imot en klarert kontaktinvitasjon.

klarert kontaktinvitasjon En e-postmelding som sendes til en person og spør om de vil bli en klarert kontakt.

klarert kontaktliste En liste over klarerte kontakter.

klarert kontaktmottaker En person som mottar en invitasjon til å bli en klarert kontakt.

klarert melding En kommunikasjonsøkt der klarerte meldinger sendes fra en klarert avsender til en klarert kontakt.

konsoll En sentral plassering hvor du får tilgang til og kan administrere funksjoner og innstillinger i HP ProtectTools Administrative Console (administrasjonskonsoll).

kryptering En prosedyre, for eksempel bruk av en algoritme, som benyttes under kryptografi for å konvertere vanlig tekst til kodet tekst for å hindre at uautoriserte mottakere leser dataene. Det finnes mange typer datakryptering, og de er basisen i nettverkssikkerhet. Vanlige typer omfatter DES (Data Encryption Standard) og PKI (Public Key Infrastructure).

kryptografi Å kryptere og dekryptere data slik at de bare kan dekodes av bestemte personer.

kryptografitjeneste (CSP - Cryptographic Service Provider) Leverandør av eller bibliotek over krypteringsalgoritmer som kan brukes i et godt definert grensesnitt for å utføre bestemte krypteringsfunksjoner.

Live Messenger History Viewer (loggvisning) En chattekomponent for Privacy Manager (personvern) som gjør det mulig å søke etter og vise krypterte chattelogger.

makulere Utføring av en algoritme som tilslører dataene i aktiva.

makuleringsprofil En angitt slettemetode og liste over aktiva.

makuleringssyklus Hvor mange ganger makuleringsalgoritmen utføres på aktiva. Jo høyere antall makuleringssykluser du velger, desto sikrere er datamaskinen.

manuell makulering Umiddelbar makulering av utvalgte aktiva, som skjer utenom den automatiske makuleringsplanen.

migrering En handling som muliggjør administrasjon, gjenoppretting og overføring av sertifikater for Privacy Manager (personvern) og klarerte kontakter.

nettverkskonto Windows-bruker eller -administratorkonto, enten på en lokal datamaskin, i en arbeidsgruppe eller på et nettverksdomene.

omstart Prosessen med å starte datamaskinen på nytt.

PIN-kode Personlig identifikasjonsnummer.

PKI Public Key Infrastructure-standard som definerer grensesnittene for oppretting, bruk og administrasjon av sertifikater og kryptografiske nøkler.

Privacy Manager-sertifikat Et digitalt personvernsertifikat som krever godkjenning hver gang du bruker det til kryptografiske operasjoner, som signering og kryptering av e-postmeldinger og Microsoft Office-dokumenter.

PSD Personlig, sikker stasjon, som sørger for et beskyttet lagringsområde for sensitiv informasjon.

pålogging Metode som en bruker benytter for å bevise sin rett til å utføre en bestemt oppgave, under en godkjenningsprosess.

påloggingsinformasjon Et objekt i Security Manager (sikkerhetsbehandling) som består av brukernavn og passord (og kanskje annen utvalgt informasjon) og som kan brukes til å logge seg på nettsteder og andre programmer.

SATA-enhetsmodus Dataoverføringsmodus mellom en datamaskin og masselagringsenheter, som harddisker og optiske stasjoner.

scene Et fotografi av en registrert bruker som skal brukes til godkjenning.

Send Security-knapp En programknapp som vises på verktøylinjen til e-postmeldinger i Microsoft Outlook. Ved å klikke på knappen kan du signere og/eller kryptere e-postmeldinger i Microsoft Outlook.

sertifiseringsmyndighet En tjeneste som utsteder sertifikatene som kreves for å bruke en PKI-infrastruktur.

Sign and Encrypt-knapp En programknapp som vises på verktøylinjen til Microsoft Office-programmer. Ved å klikke på knappen kan du signere, kryptere eller fjerne krypteringen av Microsoft Office-dokumenter.

signaturlinje En plassholder for visuell visning av en digital signatur. Når et dokument signeres, vises navnet på den som undertegner og bekreftelsesmetoden. Signeringsdatoen og tittelen til den som undertegner kan også være inkludert.

sikkerhetskopiere Bruk av sikkerhetskopifunksjonen til å lagre en kopi av viktig programinformasjon på et sted utenfor programmet. Den kan brukes til å gjenopprette informasjonen på den samme eller en annen datamaskin på et senere tidspunkt.

sikkerhetspåloggingsmetode Metoden du bruker til å logge deg på datamaskinen.

Single Sign On (engangspålogging) Funksjon som lagrer godkjenningsinformasjon og gjør det mulig å bruke Security Manager (sikkerhetsbehandling) til å få tilgang til Internett og Windows-programmer som krever passordgodkjenning.

smartkort En liten maskinvaredel som i størrelse og form ligner på et kredittkort, som lagrer identifiserende informasjon om eieren. Brukes til å godkjenne eieren av en datamaskin.

tastsekvens En kombinasjon av bestemte taster som når de trykkes, starter en automatisk makulering, for eksempel ctrl+alt+s.

tilbakekallingspassord Et passord som opprettes når en bruker anmoder om et digitalt sertifikat. Passordet kreves når brukeren ønsker å tilbakekalle sitt digitale sertifikat. Det sørger for at bare brukeren kan tilbakekalle sertifikatet.

tilgangskontrollpolicy for enheter Listen over enheter som en bruker er gitt eller nektet tilgang til.

token Se sikkerhetspåloggingsmetode.

TXT Trusted Execution Technology.

USB-token Sikkerhetsenhet som lagrer identifikasjonsopplysninger om en bruker. Akkurat som et Java-kort eller en biometrisk leser brukes den til å godkjenne eieren av en datamaskin.

Windows-administrator En bruker med fulle rettigheter til å endre tillatelser og administrere andre brukere.

Windows-brukerkonto Profil for en enkeltperson som er autorisert til å logge på et nettverk eller en enkeltstående datamaskin.

Windows-påloggingssikkerhet Beskytter Windows-konti ved å kreve bruk av bestemt påloggingsinformasjon for å få tilgang.

virtuelt token Sikkerhetsfunksjon som fungerer omtrent som et Java-kort og en kortleser. Tokenet lagres enten på datamaskinens harddisk eller i Windows-registeret. Når du logger deg på med et virtuelt token, blir du bedt om en bruker-PIN-kode for å fullføre godkjenningen.

Stikkordregister