HP Client Security

Introduktion

Første udgave: August 2013

Dokumentets bestillingsnummer: 735339-081

Indholdsfortegnelse

1 Introduktion til HP Client Security Manager

HP Client Sikkerhed giver dig mulighed for at beskytte dine data, enheder og identitet, hvorved sikkerheden på din computer forøges.

De tilgængelige softwaremoduler til din computer kan variere afhængigt af hvilken model du har.

HP Client Security-softwaremoduler kan være forudinstalleret, forudindlæst eller kan hentes fra HP's websted. Yderligere oplysninger finder du i http://www.hp.com.

BEMÆRK: Instruktionerne i denne vejledning er skrevet under den forudsætning, at du allerede har installeret de relevante HP Client Security-softwaremoduler.

HP Client Security-funktioner

Følgende tabel viser de vigtigste funktioner i HP Client Security-modulerne.

Modul	Vigtigste funktion
Brug af HP Client Security Manager	Administratorer kan udføre følgende funktioner: • Beskytte din computer før Windows® starter • Beskytte din Windows-konto med sikker godkendelse • Administrere dit logon og dine adgangskoder til websider og programmer • Nemt ændre adgangskode til dit Windows operativsystem • Benytte fingeraftryk for ekstra sikkerhed og brugervenlighed • Opsætte et chipkort, kontaktløst kort eller nærhedskort til brug ved godkendelse • Bruge din Bluetooth-telefon som en metode til identifikation • Indstille en PIN-kode for at udvide din valgmuligheder i forbindelse med godkendelse • Konfigurere logon- og sessionpolitikker • Sikkerhedskopiere og gendanne programdata • Tilføje flere programmer, såsom HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager, og HP Computrace Almindelige brugere kan udføre følgende funktioner: • Få vist indstillinger for krypteringsstatus og Device Access Manager. • Aktivere Computrace. • Konfigurere præferencer og sikkerhedskopi samt genoprettelsesindstillinger.

Modul	Vigtigste funktion
Password Manager	Almindelige brugere kan udføre følgende funktioner: • Organiser og opsæt brugernavne og adgangskoder. • Skab stærkere adgangskoder for bedre kontosikkerhed for e-mail- og web-konti. Password Manager udfylder og sender oplysningerne automatisk. • Strømlin log ind-proces med funktionen Single Sign On (Enkelt sign-on), som automatisk husker og anvender legitimationsoplysninger for bruger. • Markér en konto som kompromitteret, så du vil blive underrettet om andre konti med tilsvarende legitimationsoplysninger. • Importér login-data fra en understøttet browser.
HP Drive Encryption (kun udvalgte modeller)	• Giver komplet kryptering af hele harddisken. • Tving før start-godkendelse for at dekryptere og få adgang til data. • Giver mulighed for at aktivere selv-krypterende drev (kun udvalgte modeller).
HP Device Access Manager	• Gør det muligt for IT-chefen at styre adgang til enheder på grundlag af brugerprofiler. • Forhindrer uautoriserede brugere i at fjerne data med eksterne lagermedier, og fra vi overføre virus til systemet fra eksterne medier. • Gør det muligt for administratorer at deaktiver adgang til kommunikationsenheder for bestemte personer eller grupper af brugere.
HP Trust Circles	• Giver fil- og dokumentsikkerhed. • Krypterer filer placeret i de brugerdefinerede mapper og beskytter dem i en tillidscirkel. • Gør det muligt at filer kun bruges og deles af medlemmer i den tillidscirkel.
Tyveri-gendannelse (Computrace, købes separat)	• Kræver separat køb af abonnementer til sporing for at kunne aktivere. • Sørger for sikker sporing af aktiver. • Overvåger brugeraktivitet samt hardware- og softwareændringer. • Vil fortsat være aktiv selv hvis harddisken omformateres eller udskiftes.

HP Client Security produktbeskrivelse og almindelige eksempler på brug

Det fleste HP Client Security-produkter har både brugergodkendelse (som regel en adgangskode) og en administrativ sikkerhedskopi for at kunne få adgang, hvis adgangskoder går tabt, ikke er tilgængelige, glemmes eller hvis virksomhedens sikkerhedsafdeling kræver adgang.

BEMÆRK: Nogle HP Client Security-produkter er udviklet til at begrænse adgangen til data. Data bør være krypteret, når det er så vigtigt, at den pågældende bruger hellere vil miste data end se det kompromitteret. Det anbefales, at alle data sikkerhedskopieres til et sikkert sted.

Password Manager

Password Manager lagrer brugernavne og adgangskoder og kan bruges til at:

- Gemme login-navne og adgangskoder der giver adgang til internettet eller e-mail.
- Automatisk logge brugeren ind på et websted eller e-mail.
- Administrere og organisere godkendelser.
- Vælge en web- eller netværksressource og få direkte adgang til det pågældende link.
- Få vist navne og adgangskoder når det er nødvendigt.
- Markér en konto som kompromitteret, så du vil blive underrettet om andre konti med tilsvarende legitimationsoplysninger.
- Importér login-data fra en understøttet browser.

Eksempel 1: En indkøber for en stor producent udfører de fleste af sine selskabstransaktioner over internettet. Hun besøger også ofte flere populære websteder, der kræver login-oplysninger. Hun er meget bevidst om sikkerhed, og bruger derfor ikke den samme adgangskode til alle konto. Indkøberen har valgt at anvende Password Manager til at matche linksene med forskellige brugernavne og adgangskoder. Når hun går ind på et websted for at logge på, viser Password Manager automatisk legitimationsoplysningerne. Hvis hun ønsker at få vist brugernavne og adgangskoder, kan Password Manager konfigureres til at vise dem.

Password Manager kan også bruges til at håndtere og organisere godkendelser. Dette værktøj giver en bruger mulighed for at vælge en web- eller netværksressource og få direkte adgang til det pågældende link. Brugeren kan også se brugernavne og adgangskoder, når det er nødvendigt.

Eksempel 2: Et hårdtarbejdende medarbejder er blevet forfremmet og vil nu være ansvarlig for hele økonomiafdelingen. Teamet skal logge på et stort antal klient web-konti, som hver bruger forskellige login-oplysninger. Disse login-oplysninger skal deles med andre medarbejdere, så fortrolighed er et problem. Medarbejderen beslutter at organisere alle linksene, firma-brugernavne og adgangskoder i Password Manager. Når arbejdet er færdigt, udleverer medarbejderen Password Manager til de ansatte, så de kan arbejde på web-konti uden at kende de legitimationsoplysninger til login, som de bruger.

HP Drive Encryption (kun udvalgte modeller)

HP Drive Encryption bruges til at begrænse adgang til data på hele computerens harddisk eller et sekundært drev. Drive Encryption kan også håndtere selv-kryptering af drev.

Eksempel 1: En læge ønsker at sikre, at det kun er ham selv, som har adgang til data på computerens harddisk. Lægen aktiverer Drive Encryption, som kræver før start-godkendelse før Windows-login. Når det er sat op, er der ingen adgang til harddisken uden en adgangskode, før operativsystemet starter. Lægen kan styrke drevsikkerheden yderligere ved at vælge at kryptere data med muligheden for selv-kryptering af drevet.

Eksempel 2: En hospitalsadministrator har brug for at sikre, at kun læger og godkendte medarbejdere kan få adgang til data på deres lokale computer uden at skulle dele deres personlige adgangskoder. IT-afdelingen tilføjer administratoren, læger og alle godkendte medarbejdere som Drive Encryption-brugere. Nu kan kun godkendte medarbejdere kan starte computeren eller domænet ved hjælp af deres personlige brugernavn og adgangskode.

HP Device Access Manager (kun udvalgte modeller)

HP Device Access Manager gør det muligt for en administrator at begrænse og administrere adgang til hardware. Device Access Manager kan bruges til at spærre uautoriseret adgang til USB flashdrev, hvor data kan kopieres. Programmet kan også bruges til at begrænse adgangen til cd/dvd-drev, kontrollere USB-enheder, netværksforbindelser osv. Et eksempel kunne være en situation, hvor eksterne leverandører har brug for adgang til virksomhedens computerudstyr, men ikke må være i stand til at kopiere data til et USB-drev.

Eksempel 1: En leder i en virksomhed som leverer medicinsk udstyr arbejder ofte med personlig helbredsoplysninger sammen med sine virksomhedsoplysninger. Medarbejderne skal have adgang til disse data, men det er meget vigtigt, at dataene ikke fjernes fra computeren med et USB-drev eller andre eksterne lagermedier. Netværket er sikkert, men computerne har cd-brændere og USB-porte, der gør det muligt at kopiere eller stjæle data. Lederen bruger Device Access Manager til at deaktivere USB-porte og cd-brændere, så de kan ikke bruges. Selvom USB-portene er låste, vil mus og tastaturer fortsat fungere.

Eksempel 2: Et forsikringsselskab ønsker at forhindre, at de ansatte kan installere eller indlæse personlig software eller data fra hjemmet. Nogle af de ansatte skal have adgang til USB-porten på alle computere. IT-chefen bruger Device Access Manager til at aktivere adgang for bestemte medarbejderne, og samtidig blokere for eksterne adgang for andre.

Computrace (købes separat)

Computrace (købes separat) er en tjeneste, der kan spore placeringen af stjålet en computer, når brugeren opretter forbindelse til internettet. Computrace kan også hjælpe med at styre og finde computere, samt overvåge brug af computere og programmer.

Eksempel 1: En skoleinspektør har givet IT-afdelingen besked på at holde styr på alle computere på skolen. Efter en indledende optælling registrerede IT-administratoren alle computere med Computrace, så de kunne spores i tilfælde af, at de nogensinde blev stjålet. For nylig opdagede skolen, at flere computere manglede, så IT-administratoren underrettede myndighederne og Computrace-funktionærer. Computerne blev fundet og tilbageleveret af myndighederne.

Eksempel 2: En ejendomsvirksomhed har brug for at administrere og opdatere computere over hele verden. De bruge Computrace til at overvåge og opdatere computere uden at skulle sende en IT-medarbejder til hver enkelt computer.

Opnå vigtige sikkerhedsmål

HP Client Security-moduler kan arbejde sammen for at tilbyde løsninger til mange forskellige sikkerhedsproblemer, herunder følgende vigtige sikkerhedsmål:

- Beskyttelse mod målrettet tyveri
- Begrænse adgang til følsomme data
- Forhindre uautoriseret adgang fra interne eller eksterne steder
- Skabe en stærk adgangskodepolitik

Beskyttelse mod målrettet tyveri

Et eksempel på målrettet tyveri ville være tyveri af en computer med fortrolige data og kundeoplysninger ved sikkerhedskontrollen i en lufthavn. Følgende funktioner hjælper med at beskytte imod målrettet tyveri:

- Funktionen før start-godkendelse hjælper, hvis den er aktiveret, med til at forhindre adgang til operativsystemet.
  - HP Client Security—Se HP Client Security på side 12.
  - HP Drive Encryption—Se HP Drive Encryption (kun udvalgte modeller) på side 29.
- Kryptering er med til at sikre, at der ikke er adgang til data selv hvis harddisken fjernes og sættes i at ikke-sikkert system.
- Computrace kan spore, hvor computeren befinder sig efter et tyveri.
  - Computrace—Se Tyveri-gendannelse (kun udvalgte modeller) på side 53.

Begrænse adgang til følsomme data

Lad os antage at en ekstern revisor arbejder på stedet og har fået computeradgang for gennemgå følsomme økonomiske data. Du ønsker ikke at revisor skal kunne udskrive filerne eller gemme dem på en skrivbar enhed, f.eks. en cd. Følgende funktioner er med til at begrænse adgang til data:

- HP Device Access Manager gør det muligt for IT-chefen for at begrænse adgangen til kommunikationsenhederne, så følsomme oplysninger ikke kan kopieres fra harddisken. Se Systemvisning på side 43.

Forhindre uautoriseret adgang fra interne eller eksterne steder

Uautoriseret adgang til en ikke-sikker forretningscomputer udgør en yderst reel risiko for virksomhedsnetværksressourcer, f.eks. finansielle oplysninger eller forsknings- og udviklingsafdelingen, og til private oplysninger, f.eks. patientjournaler poster eller personlige finansielle optegnelser. Følgende funktioner hjælp til at forhindre uautoriseret adgang:

- Funktionen før start-godkendelse hjælper, hvis den er aktiveret, med til at forhindre adgang til operativsystemet. (se HP Drive Encryption (kun udvalgte modeller) på side 29.
- HP Client Security er med til at sikre, at en uautoriseret bruger ikke kan få fat i adgangskoder eller adgang til adgangskodebeskyttede programmer. Se HP Client Security på side 12.
- HP Device Access Manager gør det muligt for IT-chefen for at begrænse adgangen til skrivbare enheder, så følsomme oplysninger ikke kan kopieres fra harddisken. Se HP Device Access Manager (kun udvalgte modeller) på side 42.

Skabe en stærk adgangskodepolitik

Hvis en firmapolitik træder i kraft, der kræver brug af en stærk adgangskodepolitik for snesevis af webbaserede programmer og databaser, giver Password Manager et beskyttet opbevaringssted for adgangskoder og et praktisk Enkelt log ind. Se Password Manager på side 18.

Yderligere sikkerhedselementer

Tildeling af sikkerhedsroller

I forbindelse med administration af computersikkerhed (især ved store organisationer) er det en vigtig praksis at opdele ansvar og rettigheder blandt forskellige typer administratorer og brugere.

BEMÆRK: I en lille organisation eller til individuel brug kan disse roller alle ligge hos den samme person.

For HP Client Security kan sikkerhedsopgaver og -rettigheder inddeles i følgende roller:

- Sikkerhedsmedarbejder - Definerer sikkerhedsniveauet for virksomheden eller netværket og bestemmer hvilke sikkerhedsfunktioner som skal anvendes, f.eks. Drive Encryption.

  BEMÆRK: Mange af funktionerne i HP Client Security kan tilpasses af sikkerhedsmedarbejderen i samarbejde med HP. Yderligere oplysninger finder du i http://www.hp.com.

- IT-administrator - Installerer og håndterer sikkerhedsfunktioner defineret af sikkerhedsmedarbejderen. Kan også aktivere og deaktivere visse funktioner. Hvis sikkerhedsmedarbejderen f.eks. har besluttet at anvende chipkort, kan IT-administratoren aktivere både adgangskode og chipkort-tilstand.

- Bruger - Bruger sikkerhedsfunktionerne. Hvis sikkerhedsmedarbejderen og IT-administratoren for eksempel har aktiveret chipkort for systemet, kan brugeren angive PIN-koden til chipkortet og bruge kortet til godkendelse.

FORSIGTIG: Administratorer opfordres til at følge “bedst praksis”, når det handler om at begrænse slutbrugerrettigheder og begrænse brugeradgang.

Uautoriserede brugere bør ikke tildeles administratorrettigheder.

Styring af HP Client Security-adgangskoder

De fleste af HP Client Security-funktionerne er beskyttet af adgangskoder. Følgende tabel indeholder de mest brugte adgangskoder, softwaremodulet hvor adgangskoden er angivet samt adgangskodens funktion.

Adgangskoderne som kun indstilles og anvendes af IT-administratorer er også anført i denne tabel. Alle andre adgangskoder kan indstilles af almindelige brugere eller administratorer.

HP Client Security-adgangskode	Indstilles i følgende modul	Funktion
Adgangskode til Windows-logon	Windows kontrolpanelet eller HP Client Security	Kan anvendes til manuel login og til godkendelse af adgang til forskellige funktioner i HP Client Security.
HP Client Security sikkerhedskopiering og gendannelse af adgangskode	HP Client Security, af den enkelte bruger	Beskytter adgangen til HP Client Security sikkerhedskopi- og gendannelsesfil.
PIN-kode til chipkort	Credential Manager	Kan bruges som multifactor-godkendelse. Kan bruges som Windows-godkendelse. Godkender brugere af Drive Encryption, hvis chipkortet er valgt.

Oprettelse af en sikker adgangskode

Når du opretter adgangskoder, skal du først følge eventuelle specifikationer, der kræves af programmet. Generelt bør du følge disse retningslinjer for at hjælpe dig med at skabe stærke adgangskoder og reducere risikoen for, at din adgangskode blive kompromitteret:

- Brug adgangskoder med mere end 6 tegn og helst mere end 8.
- Bland store og små bogstaver i hele din adgangskode.
- Når det er muligt skal du indsætte alfanumeriske tegn og inkludere specialtegn og tegnsætningstegn.
- Indsæt specialtegn eller numre i stedet for bogstaver i et nøgleord. Du kan f.eks. bruge nummer 1 til bogstaverne I eller L.
- Kombiner ord fra 2 eller flere sprog.
- Opdel et ord eller sætning med numre eller specialtegn i midten, f.eks. “Mary2-2CAT45.”
- Brug ikke en adgangskode som ville blive vist i en ordbog.
- Brug ikke dit navn som adgangskode og andre personlige oplysninger, såsom din fødselsdag, navne på kæledyr eller din mors pigenavn, selv hvis du staver det bagvendt.
- Ændr adgangskoder regelmæssigt. Du kan nøjes med at ændre et par tegn, der stiger.
- Hvis du skriver din adgangskode ned, må du ikke gemmer den på et almindeligt synligt sted tæt på computeren.
- Gem ikke adgangskoden i en fil, f.eks. en e-mail, på computeren.
- Undlad at dele konti eller give andre din adgangskode.

Sikkerhedskopiering af legitimationsoplysninger og indstillinger

Du kan bruge sikkerhedskopierings- og gendannelsesværktøjet i HP Client Security som en central placering, hvorfra du kan sikkerhedskopiere og gendanne legitimationsoplysninger til sikkerhed for nogle af de installerede HP Client Security-moduler.

2 Sådan kommer du i gang

Start HP Client Security på en af følgende måder, for at konfigurere HP Client Security til brug med dine legitimationsoplysninger. Når guiden er blevet gennemført af en bruger, kan den ikke startes igen af den pågældende bruger.

1. Fra Start- eller App-skærmen klikkes eller trykkes på appen **HP Client Security** (Windows 8).

   - eller -

   Fra Windows-skrivebordet klikkes eller trykkes på **HP Client Security Gadget** (Windows 7).

   - eller -

   Fra Windows-skrivebordet, dobbeltklik eller dobbelttryk på ikonet **HP Client Security** i meddelelsesområdet, som er placeret længst til højre på proceslinjen.

   - eller -

   Fra Windows-skrivebordet, klikkes eller trykkes på ikonet **HP Client Security** i meddelelsesområdet, hvorefter **Open HP Client Security** vælges.

2. Guiden HP Client Security Setup starter, og velkomstsiden vises.

3. Læs velkomstskærmen, verificer din identitet ved at indtaste din adgangskode til Windows, og klik eller tryk derefter på **Næste**.

   Hvis du endnu ikke har oprettet en Windows-adgangskode, bliver du bedt om at oprette en. En adgangskode til Windows er påkrævet for at beskytte din Windows-konto mod uautoriserede personers adgang og for at benytte funktionerne i HP Client Security.

4. Vælg tre sikkerhedsspørgsmål på siden HP SpareKey. Indtast et svar til hvert enkelt spørgsmål og klik derefter på **Næste**. Brugerdefinerede spørgsmål er også tilladt. Se HP SpareKey—Gendannelse af adgangskode på side 14 for at få flere oplysninger.

5. På siden Fingeraftryk registreres som et minimum det mindste tilladte antal fingeraftryk, hvorefter der klikkes eller trykkes på **Næste**. Se Fingeraftryk på side 12 for at få flere oplysninger.

6. Aktiver kryptering på siden Drive Encryption (Drevkryptering), sikkerhedskopier krypteringsnøglen, og klik eller tryk på **Næste**. Se HP Drive Encryption software-hjælp for flere oplysninger.

   BEMÆRK: Dette gælder for situationer hvor brugeren er en administrator, og hvor guiden HP Client Security Setup ikke forudgående er blevet konfigureret af en administrator.

7. Klik eller tryk på **Afslut** på guidens sidste side.

   Denne sider giver en status over funktioner og legitimationsoplysninger.

8. Opsætningsguiden HP Client Security Setup sørger for at Just In Time-godkendelse og File Sanitizer-funktionerne aktiveres. Se HP Device Access Manager software-hjælp og HP File Sanitizer software-hjælp for flere oplysninger.

   BEMÆRK: Dette gælder for situationer hvor brugeren er en administrator, og hvor guiden HP Client Security Setup ikke forudgående er blevet konfigureret af en administrator.

Sådan åbnes HP Client Security

Du kan åbne programmet HP Client Security på en af følgende måder:

BEMÆRK: Opsætningsguiden HP Client Security skal være fuldført, før programmet HP Client Security kan startes.

- Fra Start- eller App-skærmen klikkes eller trykkes på appen **HP Client Security**.

  - eller -

  Fra Windows-skrivebordet klikkes eller trykkes på **HP Client Security Gadget** (Windows 7).

  - eller -

  Fra Windows-skrivebordet, dobbeltklik eller dobbelttryk på ikonet **HP Client Security** i meddelelsesområdet, som er placeret længst til højre på proceslinjen.

  - eller -

  Fra Windows-skrivebordet, klikkes eller trykkes på ikonet **HP Client Security** i meddelelsesområdet, hvorefter **Open HP Client Security** vælges.

3 Nem Installationsvejledning til små virksomheder

Dette kapitel er designet til at vise de grundlæggende trin, der kræves for at aktivere de mest almindelige og nyttige indstillinger i HP Client Security for små virksomheder. Adskillige værktøjer og indstillinger i denne software giver dig mulighed for at fintune dine præferencer og indstille din adgangskontrol. Fokus i denne nemme installationsvejledning er på at få hvert modul op at køre med mindst mulig indsats og tid brugt på opsætning. For yderligere oplysninger skal du vælge modulet, du er interesseret i og derefter klikke på **?** eller Hjælp-knappen i øverste højre hjørne. Denne knap viser automatisk oplysninger på skærmen, som hjælper dig med det aktuelt viste vindue.

Sådan kommer du i gang

1. Fra Windows-skrivebordet skal du åbne HP Client Security ved at dobbeltklikke på ikonet **HP Client Security** i meddelelsesområdet placeret yderst til højre på proceslinjen.
2. Indtast din Windows-adgangskode eller opret en Windows-adgangskode.
3. Gennemfør opsætningen af HP Client Security.

For at få HP Client Security til kun at kræve godkendelse én gang under Windows-login, se Sikkerhedsfunktioner på side 26.

Password Manager

Vi har alle har en lang række adgangskoder – især hvis du jævnlig går ind på websteder og applikationer, der kræver, at du skal logge på. Den normale bruger anvender enten den samme adgangskode til alle programmer og websteder, eller bliver kreativ og glemmer hurtigt hvilken adgangskode, som passer til hvilket program.

Password Manager kan automatisk huske dine adgangskoder, eller giver dig mulighed for at skelne hvilke websteder som skal huskes, og hvilke som skal glemmes. Når du har logget på til computeren, vil Password Manager huske dine adgangskoder eller legitimationsoplysninger for programmer eller websteder som deltager.

Når du går ind i et program eller websted, der kræver legitimationsoplysninger, vil Password Manager automatisk genkende stedet og spørge, om du ønsker, at software at huske dine oplysninger. Hvis du vil ekskludere visse sites, kan du afslå anmodningen.

For at begynde at gemme websteder, brugernavne og adgangskoder:

1. Gå for eksempel til et nyt websted eller program og klik derefter på Password Manager-ikonet i øverste venstre hjørne af websiden for at tilføje web-godkendelse.
2. Navngiv linket (valgfrit) og indtast et brugernavn og en adgangskode i Password Manager.
3. Når du er færdig, skal du klikke på **OK**-knappen.
4. Password Manager kan også gemme dit brugernavn og adgangskoder til delte netværk eller mapper på netværksdrev.

Visning af og administration af gemte godkendelser i Password Manager

Password Manager giver dig mulighed for at se, administrere, sikkerhedskopiere og starte dine godkendelser fra ét centralt sted. Password Manager understøtter også start af gemte steder fra Windows.

For at åbne Password Manager: brug tastaturkombinationen Ctrl+Windows-tasten+h for at åbne Password Manager, og klik derefter på **Log på** for at starte og godkende den gemte genvej.

Password Managers **Rediger**-indstilling giver dig mulighed for at få vist og redigere navn, login-navn og endda afsløre adgangskoderne.

Med HP Client Security til små virksomheder kan alle legitimationsoplysninger og indstillinger sikkerhedskopieres og/eller kopieres til en anden computer.

HP Device Access Manager

Device Access Manager kan bruges til at begrænse brugen af forskellige interne og eksterne lagerenheder, så dine data forbliver sikret på harddisken, og ikke forlader din virksomhed. Et eksempel kunne være for at tillade en bruger adgang til dine data, men samtidig at forhindre ham/hende i at kopiere dataene til en cd, musikafspiller eller USB-hukommelsesenhed.

1. Åbn **Device Access Manager** (se Åbning af HP Device Access Manager på side 42).

   Adgang for den aktuelle bruger vises.

2. For at ændre adgang for brugerne, grupper eller enheder, klik eller tryk på ***Ændr***. Se Systemvisning på side 43 for at få flere oplysninger.

HP Drive Encryption

HP Drive Encryption bruges til at beskytte dine data ved at kryptere hele harddisken. Dataene på din harddisk vil blive ved med at være beskyttede, hvis din pc er nogensinde bliver stjålet, og/eller hvis harddisken bliver fjernet fra den oprindelige computer og sættes i en anden computer.

En yderligere sikkerhedsfordel er, at Drive Encryption kræver korrekt godkendelse vha. dit brugernavn og adgangskode, før operativsystemet starter. Denne proces kaldes før start-godkendelse.

For at gøre det nemt for dig vil flere softwaremoduler synkronisere adgangskoder automatisk, inklusive Windows-brugerkonti, godkendelsesdomæner, HP Drive Encryption, Password Manager og HP Client Security.

For konfigurering af HP Drive Encryption under startopsætning med opsætningsguiden til HP Client Security, se Sådan kommer du i gang på side 8.

4 HP Client Security

HP Client Security startsiden er det centrale sted, hvor man nemt kan få adgang til funktioner, programmer og indstillinger, som hører til HP Client Security. Startsiden er delt op i tre sektioner:

- **DATA**—Giver adgang til programmer som benyttes til administration af datasikkerhed.
- **ENHED**—Giver adgang til programmer som benyttes til administration af enhedssikkerhed.
- **IDENTITET**—Benyttes til registrering og administration af godkendelsesoplysninger.

Placer markøren over et program-felt for at få vist en beskrivelse af programmet.

HP Client Security giver muligvis links til bruger- og administratorindstillinger nederst på en side. HP Client Security giver adgang til avancerede indstillinger og funktioner ved at man klikker eller trykker på ikonet **Gear** (indstillinger).

Identitetsfunktioner, programmer og indstillinger

De identitetsfunktioner, programmer og indstillinger som HP Client Security byder på, hjælper dig til at administrere forskellige aspekter af din digitale identitet. Klik eller tryk på et af de følgende felter på HP Client Security startsiden og indtast derefter din adgangskode til Windows:

- **Fingeraftryk**—Registrerer og administrerer legitimationsoplysninger i forbindelse med dit fingeraftryk.
- **SpareKey**—Opsætter og administrerer din HP SpareKey legitimationsoplysning, som kan bruges til at logge ind på din computer hvis andre legitimationsoplysninger er gået tabt eller er blevet forlagt. Her kan du også nulstille din glemte adgangskode.
- **Adgangskode til Windows**—Giver nem adgang til at ændre din adgangskode til Windows.
- **Bluetooth-enheder**—Her kan du registrere og administrere dine Bluetooth-enheder.
- **Kort**—Her kan du registrere og administrere dine chipkort, kontaktløse kort og nærhedskort.
- **PIN**—Her kan du registrere og administrere dine PIN-legitimationsoplysninger.
- **RSA SecurID**—Giver dig mulighed for at registrere og håndtere dine RSA SecurID legitimationsoplysninger (hvis korrekt opsætning er foretaget).
- **Password Manager** (Adgangskode-administration)—Her kan du administrere adgangskoder for dine onlinekonti og programmer.

Fingeraftryk

Opsætningsguiden HP Client Security Setup vejleder dig gennem opsætning, eller "registrering", af dine fingeraftryk.

Du kan også registrere eller slette dine fingeraftryk på siden Fingeraftryk, som du får adgang til ved at klikke eller trykke på ikonet **Fingeraftryk** på HP Client Security startsiden.

1. På siden Fingeraftryk skal du stryge en finger, indtil registreringen er gennemført.

   Det antal fingre, som er påkrævet ved registrering, angives på siden. Pegefingeren eller de midterste fingre er at foretrække.

2. For at slette fingeraftryk, som tidligere er blevet registreret, skal du klikke eller trykke på **Slet**.
3. For at registrere yderligere fingre, klik eller tryk på **Enroll an additional fingerprint** (Registrer endnu et fingeraftryk).
4. Klik eller tryk på **Gem** før siden forlades.

⚠ **FORSIGTIG:** Når fingeraftryk registreres ved hjælp af guiden, gemmes informationerne om fingeraftryk ikke før du klikker på **Næste**. Hvis computeren får lov at være inaktiv et stykke tid eller programmet lukkes, gemmes de ændringer du har foretaget **ikke**.

- For at få adgang til administrative indstillinger for fingeraftryk, hvor administratorer kan angive registrering, nøjagtighed og andre indstillinger, skal man klikke eller trykke på **Administrative indstillinger** (kræver administratorrettigheder).
- For at få adgang til bruger-indstillinger for fingeraftryk, hvor du kan angive indstillinger som styrer udseende og funktionsmåde for genkendelse af fingeraftryk, klik eller tryk på **Brugerindstillinger**.

Fingeraftryk Administrative Indstillinger

Administratorer kan angive registrering, nøjagtighed og andre indstillinger for fingeraftrykslæseren. Der kræves administratorrettigheder.

- For at få adgang til administrationsindstillingerne for fingeraftrykslegitimationsoplysningen, klik eller tryk på **Administrative Settings** (Administrationsindstillinger) på siden Fingeraftryk.

- **User enrollment** (Registrering af brugere)—Vælg det minimale eller maksimale antal fingeraftryk, som en bruger kan registrere.
- **Recognition** (Genkendelse)—Flyt skyderen for at justere den følsomhed fingeraftrykslæseren har, når du stryger din finger.

  Hvis dit fingeraftryk ikke genkendes hver gang, er det måske nødvendigt af vælge en lavere indstilling for genkendelse. En højere indstilling øger følsomhed over for variationer i fingeraftryks-strygninger og formindsker derfor muligheden for fejlagtig godkendelse. Indstillingen **Medium-High** (Mellem-Høj) giver en god blanding af brugbarhed og sikkerhed.

Fingeraftryk brugerindstillinger

På siden Fingerprint User Settings (Fingeraftryk brugerindstillinger) kan du angive indstillinger, som styrer udseende og funktionsmåde for genkendelse af fingeraftryk.

▲ For at få adgang til brugerindstillingerne for fingeraftrykslegitimationsoplysningen, klik eller tryk på **User Settings** (Brugerindstillinger) på siden Fingeraftryk.

- **Aktiver lyd-feedback**—Som standard giver HP Client Security dig lyd-feedback når et fingeraftryk er blevet strøget, og afspiller forskellige lyde for forskellige programhændelser. Du kan tildele nye lyde til disse hændelser under fanen Lyde i indstillingen Lyde i Windows kontrolpanelet, eller du kan deaktivere lyd-feedback ved at rydde afkrydsningsfeltet.
- **Show scan quality feedback** (Vis feedback om scanningens kvalitet)—Vælg afkrydsningsfeltet for at vise alle strygninger, uanset deres kvalitet. Ryd afkrydsningsfeltet for kun at vise strygninger af en god kvalitet.

HP SpareKey—Gendannelse af adgangskode

Med HP SpareKey kan du få adgang til din computer (på platforme som understøttes) ved at svare på tre sikkerhedsspørgsmål.

HP Client Security beder dig om at opsætte din personlige HP SpareKey i forbindelse med den første konfigurering i opsætningsguiden HP Client Security Setup.

For at indstille din HP SpareKey:

1. Vælg tre sikkerhedsspørgsmål på siden HP SpareKey i opsætningsguiden, og indtast derefter et svar til hvert spørgsmål.

   Du kan vælge et svar fra en foruddefineret liste eller du kan skrive dine egne spørgsmål ned.

2. Klik eller tryk på **Registrer**.

For at slette din HP SpareKey:

▲ Klik eller tryk på **Delete your SpareKey** (Slet din SpareKey).

Efter din SpareKey er blevet indstillet, kan du få adgang til din computer ved hjælp af din SpareKey på en logon-skærm til opstartsgodkendelse eller på skærmen Velkommen til Windows.

Du kan vælge forskellige spørgsmål, eller ændre dine svar på siden SpareKey, som du får adgang til via feltet Password Recovery (Gendannelse af adgangskode) på HP Client Security startsiden.

Man får adgang til HP SpareKey Settings (Indstillinger for HP Sparekey), hvor en administrator kan angive indstillinger som har at gøre med legitimationsoplysningerne til HP Sparekey, ved at klikke på **Settings** (Indstillinger) (kræver administratorrettigheder).

HP SpareKey Settings

På siden HP SpareKey Settings (Indstillinger for HP SpareKey) kan du angive indstillinger, som styrer udseende og funktionsmåde for legitimationsoplysningerne til HP SpareKey.

▲ For at åbne side HP SpareKey Settings (Indstillinger for HP SpareKey), klik eller tryk på **Indstillinger** på siden HP SpareKey (kræver administratorrettigheder).

Administratorer kan vælge følgende indstillinger:

- Angiv de spørgsmål som præsenteres for hver enkelt bruger under opsætning af HP SpareKey.
- Definer op til tre nye sikkerhedsspørgsmål, som skal føjes til den liste som præsenteres for brugerne.

- Vælg om brugerne skal have lov til at angive deres egne sikkerhedsspørgsmål eller ej.
- Vælg de godkendelses-miljøer (Windows eller opstartsgodkendelse) der skal tillade brug af HP SpareKey.

Windows-adgangskode

Med HP Client Security er det nemmere og hurtigere at ændre din adgangskode til Windows end hvis du bruger Windows kontrolpanelet.

For at ændre din adgangskode til Windows:

1. På HP Client Security startsiden, klik eller tryk på **Windows Password** (Windows-adgangskode).
2. Indtast din nuværende Windows-adgangskode i tekstfeltet **Current Windows password** (Aktuelle Windows-adgangskode).
3. Indtast en ny adgangskode i tekstfeltet **New Windows password** (Ny Windows-adgangskode) og indtast den derefter igen i tekstfeltet **Confirm new password** (Bekræft ny adgangskode).
4. Klik eller tryk på **Change** (Skift) for med øjeblikkelig virkning at skifte fra din nuværende adgangskode til den som du har indtastet.

Bluetooth-enheder

Hvis administratoren har aktiveret Bluetooth som en legitimationsoplysning, kan du skabe yderligere sikkerhed ved at opsætte en Bluetooth-telefon i sammenhæng med andre oplysninger.

BEMÆRK: Kun telefoner med Bluetooth understøttes.

1. Sørg for at Bluetooth-funktionaliteten på computeren er slået til, og at Bluetooth-telefonen er i en tilstand, hvor den kan findes. For at tilslutte telefonen, kræves det muligvis, at du på Bluetooth-enheden indtaster en kode som genereres automatisk. Alt afhængig af hvordan Bluetooth-enheden er konfigureret, er det muligvis nødvendigt at sammenligne pardannelseskoderne mellem computeren og telefonen.
2. For at registrere en telefon, vælg den og klik eller tryk derefter på **Registrer**.

For at få adgang til siden Indstillinger for Bluetooth-enheder på side 15, hvor en administrator kan angive indstillinger for Bluetooth-enheder, klik på **Indstillinger** (kræver administratorrettigheder).

Indstillinger for Bluetooth-enheder

Administratorer kan angive følgende indstillinger, som styrer udseende og funktionsmåde for Bluetooth-legitimationsoplysninger:

Silent Authentication (Godkendelse i baggrunden)

- **Brug automatisk din tilsluttede og registrerede Bluetooth-enhed i forbindelse med bekræftelse af din identitet**—Vælg afkrydsningsfeltet for at gøre det muligt for brugerne at benytte Bluetooth-registreringsoplysninger til godkendelse, uden at der kræves handling fra brugerens side, eller ryd afkrydsningsfeltet for at deaktivere denne mulighed.

Bluetooth Proximity (Bluetooth-nærhed)

- **Lås computeren når din registrerede Bluetooth-enhed flytter sig uden for rækkevidde af computeren**—Marker afkrydsningsfeltet for at låse computeren når en Bluetooth-enhed, der

blev tilsluttet ved login, flytter sig uden for området, eller fjern markeringen i afkrydsningsfeltet for at deaktivere denne indstilling

BEMÆRK: Bluetooth-modulet på din computer skal understøtte denne funktionalitet, for at denne funktion kan benyttes.

Kort

HP Client Security kan understøtte et udvalg af forskellige identifikationskort, som er små plastic-kort med en indbygget computer-chip. De omfatter chipkort, kontaktløse kort og nærhedskort. Hvis et af disse kort og en passende læser forbindes til computeren, hvis administratoren har installeret den tilhørende driver fra producenten, og hvis administratoren har aktiveret kortet som en godkendelsesoplysning, kan du benytte kortet som en godkendelsesoplysning.

I forbindelse med chipkort, bør producenten levere værktøjer til at installere det sikkerhedscertifikat og den PIN-administration, som HP Client Security bruger i sin sikkerheds-algoritme. Antallet og typen af tegn, som benyttes i PIN-koden kan variere. En administrator skal initialisere chipkortet før det kan bruges.

Følgende chipkort-formater understøttes af HP Client Security:

- CSP (Program til kryptografiske tjenester)
- PKCS11

Følgende formater for kontaktløse kort understøttes af HP Client Security:

- Kontaktløse HID iCLASS hukommelseskort
- Kontaktløse MiFare Classic 1k, 4k, og mini-hukommelseskort

Følgende formater for nærhedskort understøttes af HP Client Security:

- HID nærhedskort

For at registrere et chipkort:

1. Sæt kortet i en tilsluttet chipkortlæser.
2. Når kortet genkendes, indtast kortets PIN-kode og klik eller tryk derefter på **Registrer**.

For at ændre PIN-koden til et chipkort:

1. Sæt kortet i en tilsluttet chipkortlæser.
2. Når kortet genkendes, indtast kortets PIN-kode og klik eller tryk derefter på **Authenticate** (Godkend).
3. Klik eller tryk på **Change PIN** (Skift PIN), og indtast derefter en ny PIN-kode.

For at registrere et kontaktløst kort eller et nærhedskort:

1. Placer kortet på eller meget tæt på den tilhørende læser.
2. Når kortet genkendes, klik eller tryk på **Registrer**.

For at slette et registreret kort:

1. Præsenter kortet for læseren.
2. Gælder kun for chipkort: Indtast kortets tildelte PIN-kode, og klik eller tryk derefter på **Authenticate** (Godkend).
3. Klik eller tryk på **Slet**.

Når kortet er registreret, vises detaljer vedrørende kortet under **Registrerede kort**. Når et kort slettes, fjernes det fra listen.

Man får adgang til indstillinger for nærhedskort, kontaktløse kort og chipkort, hvor administratorer kan angive indstillinger for kort-tilmeldingsoplysninger, ved at klikke eller trykke på **Settings** (Indstillinger) (kræver administratorrettigheder).

Indstillinger for nærhedskort, kontaktløse kort og chipkort

Klik eller tryk på kortet i listen og klik eller tryk derefter på den pil som vises, for at få adgang til indstillingerne for kortet.

For at ændre PIN-koden til et chipkort:

1. Præsenter kortet for læseren.
2. Indtast kortets tildelte PIN-kode, og klik eller tryk derefter på **Fortsæt**.
3. Indtast og bekræft den nye PIN-kode, og klik eller tryk derefter på **Fortsæt**.

For at initialisere PIN-koden til et chipkort:

1. Præsenter kortet for læseren.
2. Indtast kortets tildelte PIN-kode, og klik eller tryk derefter på **Fortsæt**.
3. Indtast og bekræft den nye PIN-kode, og klik eller tryk derefter på **Fortsæt**.
4. Klik eller tryk på **Ja** for at bekræfte initialiseringen.

For at slette kort-data:

1. Præsenter kortet for læseren.
2. Indtast kortets tildelte PIN-kode (gælder kun for chipkort), og klik eller tryk derefter på **Fortsæt**.
3. Klik eller tryk på **Ja** for at bekræfte sletningen.

PIN

Hvis administratoren har aktiveret en PIN-kode som en legitimationsoplysning, kan du skabe yderligere sikkerhed ved at opsætte en PIN-kode i sammenhæng med andre oplysninger.

For at indstille en ny PIN-kode:

- Indtast PIN-koden, indtast den igen for at bekræfte den, og klik eller tryk derefter på **Anvend**.

Sådan slettes en PIN-kode:

- Klik eller tryk på **Slet**, og klik eller tryk derefter på **Ja** for at bekræfte.

Man får adgang til PIN Settings (PIN-indstillinger) hvor administratorer kan angive indstillinger som har at gøre med PIN-legitimationsoplysninger, ved at klikke eller trykke på **Settings** (Indstillinger) (kræver administratorrettigheder).

PIN Settings

På siden PIN-indstillinger, kan du den minimale og maksimale acceptable længde for PIN-koden.

RSA SecurID

Hvis administratoren har aktiveret RAS som en godkendelsesoplysning, og følgende betingelser er opfyldt, kan du registrere eller slette en RSA SecurID-oplysning.

BEMÆRK: Den fornødne opsætning skal være på plads.

- Brugeren skal være oprettet på en RSA-Server.
- Det RSA SecurID token som er tildelt brugeren og computeren skal være forbundet med RSA Server-domænet.
- Softwaren skal være installeret på computeren.
- En forbindelse til den korrekt konfigurerede RSA-server skal være tilgængelig.

For at registrere en RSA SecurID legitimationsoplysning:

▲ Indtast dit RSA SecurID brugernavn og din adgangskode (RSA SecurID Token-kode eller PIN +Token-kode, alt afhængig af miljøet), og klik eller tryk derefter på **Anvend**.

Efter registreringen er gennemført, vises meddelelsen, “Your RSA SecurID credential has been successfully enrolled” (“Registrering af din RSA SecurID legitimationsoplysning er gennemført”), og knappen Slet aktiveres.

For at slette en RSA SecurID legitimationsoplysning:

▲ Klik **Slet**, og vælg derefter **Ja** i pop-op dialogen, som spørger “Are you sure you want to delete your RSA SecurID credential?” ("Er du sikker på at du ønsker at slette din RSA SecurID legitimationsoplysning?")

Password Manager

Det er lettere og mere sikkert at logge ind på websider og programmer, når du bruger Password Manager. Du kan oprette stærkere adgangskoder, som du ikke behøver at skrive ned eller huske, og derefter nemt og hurtigt logge på med et fingeraftryk, et nærhedskort, et kontaktløst kort, et chipkort, en Bluetooth-telefon, en PIN-kode, en RSA-legitimationsoplysning eller med din adgangskode til Windows.

BEMÆRK: Eftersom websiders logon-skærme konstant ændres, er det muligt at Password Manager ikke vil være i stand til at understøtte alle websider til enhver tid.

Password Manager tilbyder følgende valgmuligheder:

Password Manager-siden

- Klik eller tryk på en konto for automatisk at åbne en webside eller et program og logge på.
- Brug kategorier til at organisere dine konti.

Adgangskode-styrke

- Få et hurtig overblik, som viser om nogen af dine adgangskoder udgør en sikkerhedsrisiko.
- Når login-data tilføjes, kan du kontrollere styrken af de individuelle adgangskoder, som benyttes til websider og programmer.
- Adgangskodernes styrke vises med røde, gule eller grønne status-indikatorer.

Ikonet **Password Manager** vises i det øverste venstre hjørne af en webside eller et programs logon-skærm. Når et logon endnu ikke er blevet oprettet for pågældende webside eller program, vises et plus-tegn på ikonet.

▲ Klik eller tryk på ikonet **Password Manager** for at vise en kontekstmenu, hvor du kan vælge en af følgende muligheder:

- Tilføj [etdomæne.com] til Password Manager
- Åbn Password Manager
- Ikon-indstillinger
- Hjælp

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

Følgende valgmuligheder vises i kontekstmenuen:

- **Add [somedomain.com] to the Password Manager** (Tilføj [etdomæne.com] til Password Manager—Her kan du tilføje et logon til den nuværende logon-skærm.
- **Åbn Password Manager**—Starter Password Manager.
- **Icon Settings** (Ikon-indstillinger)—Her kan du angive betingelser, som afgør hvornår ikonet **Password Manager** vises.
- **Hjælp**—Viser HP Client Security-hjælp.

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

Følgende valgmuligheder vises i kontekstmenuen:

- **Fill in logon data** (Udfyld login-data)—Viser siden **Verify your identity** (Bekræft din identitet). Hvis godkendelse gennemføres med held, placeres dine login-data i login-felterne, hvorefter siden sendes (hvis afsendelse blev angivet da dette login blev oprettet eller sidste gang det blev redigeret).
- **Edit Logon** (Rediger logon)—Her kan du redigere dine login-data for denne webside.
- **Add Logon**—Her kan du tilføje en konto til Password Manager.
- **Åbn Password Manager**—Starter Password Manager.
- **Hjælp**—Viser HP Client Security-hjælp.

BEMÆRK: Denne computers administrator har muligvis konfigureret HP Client Security til at kræve mere end én legitimationsoplysning, når din identitet skal bekræftes.

Tilføj logons

Du kan nemt tilføje et login til en webside eller et program ved at indtaste login-oplysningerne en enkelt gang. Derefter indtaster Password Manager automatisk oplysningerne for dig. Du kan benytte disse logins efter du har fundet websiden eller programmet frem.

For at tilføje et login:

1. Åbn login-skærmen til et program eller en webside.
2. Klik eller tryk på ikonet **Password Manager**, og klik eller tryk derefter på en af følgende, alt afhængig af om login-skærmen giver adgang til en webside eller et program:
   - Hvis det er en webside, klik eller tryk på **Add [domain name] to Password Manager** (Tilføj [domænenavn] til Password Manager).
   - Hvis det er et program, klik eller tryk på **Add this logon screen to Password Manager** (Tilføj denne login-skærm til Password Manager).
3. Indtast dine logondata. Login-felter på skærmen, og de tilsvarende felter i dialogboksen, identificeres med en tyk orange kant.
   a. For at udfylde et login-felt med et af de allerede formatterede valg, skal du klikke eller trykke på pilene til højre for feltet.
   b. For at se adgangskoden til dette logon, skal du klikke eller trykke på **Show password** (Vis adgangskode).
   c. For at få udfyldt login-felterne uden at indsende oplysningerne, skal afkrydsningsfeltet **Automatically submit logon data** (Indsend login-data automatisk) ryddes.
   d. Klik eller tryk på **OK** for at vælge den godkendelsesmetode du ønsker at bruge (fingeraftryk, nærhedskort, kontaktløst kort, chipkort, Bluetooth-telefon, PIN-kode eller adgangskode), og log derefter på med den valgte godkendelsesmetode.

      Plus-tegnet fjernes fra ikonet **Password Manager** for at vise at logon-oplysningerne er blevet oprettet.
   e. Hvis Password Manager ikke opdager login-felterne, kan du klikke eller trykke på **More fields** (Flere felter).
      - Vælg afkrydsningsfeltet for hvert felt, der kræves til logon, eller ryd afkrydsningsfelterne for hvert felt, der ikke kræves til logon.
      - Klik eller tryk på **Luk**.

Hver gang du åbner pågældende webside eller program, vises ikonet **Password Manager** i øverste venstre hjørne af websiden eller programmets logon-skærm, for at indikere at du kan bruge dine registrerede legitimationsoplysninger til at logge på.

Redigering af logons

For at redigere et login:

1. Åbn login-skærmen til et program eller en webside.
2. For at vise en dialogboks, hvor du kan redigere dine login-oplysninger, klik eller tryk på ikonet **Password Manager**, og klik eller tryk derefter på **Rediger Logon**.

   Login-felter på skærmen, og de tilsvarende felter i dialogboksen, identificeres med en tyk orange kant.

   Du kan også redigere kontooplysninger ved hjælp af siden Password Manager ved at klikke eller trykke på logon'et for at vise redigeringsmulighederne, og derefter vælge **Rediger**.

3. Rediger dine login-oplysninger.

   - For at redigere **Kontonavnet**, indtast et nyt navn i feltet.
   - For at tilføje eller redigere et navn på en **Kategori** skal det indtastes eller modificeres i feltet **Kategori**.
   - For at vælge et login-felt til **Brugernavn** med et af de allerede formatterede valg, skal du klikke eller trykke på pil ned til højre for feltet.

     Allerede formatterede valg er kun tilgængelige når logon'et redigeres via kommandoen Rediger fra Password Manager-ikonets kontekstmenu.
   - For at vælge et login-felt til **Adgangskode** med et af de allerede formatterede valg, skal du klikke eller trykke på pil ned til højre for feltet.

     Allerede formatterede valg er kun tilgængelige når logon'et redigeres via kommandoen Rediger fra Password Manager-ikonets kontekstmenu.
   - For at føje yderligere felter fra skærmen til dit logon, klik eller tryk på **More fields** (Flere felter).
   - For at se adgangskoden til dette logon, skal du klikke eller trykke på **Show password** (Vis adgangskode).
   - For at få udfyldt login-felterne uden at indsende oplysningerne, skal afkrydsningsfeltet **Automatically submit logon data** (Indsend login-data automatisk) ryddes.
   - For at markere et logon, som har en adgangskode der ikke længere er sikker, skal du vælge afkrydsningsfeltet **This password is compromised** (Denne adgangskode er ikke sikker).

     Efter at indstillingen er gemt, vil alle andre logons, som har den samme adgangskode, også blive markeret som værende usikre. Du kan derefter besøge hver enkelt berørt konto og ændre adgangskoderne efter behov.

4. Klik eller tryk på **OK**.

Brug af Password Manager-menuen Quick Links (Genvejslinks)

Password Manager tilbyder en hurtig, nem måde til at åbne websider og programmer, som du har oprettet logons til. Dobbeltklik eller dobbelttryk på et logon til et program eller en webside fra menuen **Password Manager Quick Links** (Password Manager Genvejslinks), eller fra siden Password Manager i HP Client Security, for at åbne login-skærmen og udfyld derefter dine login-data.

Når du opretter et logon, føjes det automatisk til menuen **Quick Links** (Genvejslinks) i Password Manager.

For at vise menuen **Quick Links** (Genvejslinks):

▲ Tryk på **Password Manager** genvejstastkombinationen (Ctrl+Windows-tasten+h er fabriksindstillingen). For at ændre genvejstastkombinationen fra HP Client Security startsiden, klik **Password Manager**, og klik eller tryk derefter på **Indstillinger**.

Organisering af logons i kategorier

Opret en eller flere kategorier for at holde orden i dine logons.

For at tildele en kategori til et logon:

1. På HP Client Security startsiden, klik eller tryk på **Password Manager**.
2. Klik eller tryk på en konto og klik eller tryk derefter på **Rediger**.

3. Indtast et navn til kategorien i feltet **Kategori**.
4. Klik eller tryk på **Gem**.

For at fjerne en konto fra en kategori:

1. På HP Client Security startsiden, klik eller tryk på **Password Manager**.
2. Klik eller tryk på en konto og klik eller tryk derefter på **Rediger**.
3. Slet navnet på kategorien i feltet **Kategori**.
4. Klik eller tryk på **Gem**.

For at omdøbe en kategori:

1. På HP Client Security startsiden, klik eller tryk på **Password Manager**.
2. Klik eller tryk på en konto og klik eller tryk derefter på **Rediger**.
3. Rediger navnet på kategorien i feltet **Kategori**.
4. Klik eller tryk på **Gem**.

Administrering af dine logons

Password Manager gør det nemt at administrere dine login-oplysninger for brugernavne, adgangskoder og flere logon-konti fra ét centralt sted.

Dine logons vises på en liste på Password Manager-siden.

For at administrere dine logons:

1. På HP Client Security startsiden, klik eller tryk på **Password Manager**.
2. Klik eller tryk på et eksisterende logon, vælg en af de følgende muligheder, og følg derefter anvisningerne på skærmen:
   - **Rediger**—Rediger et logon. Se Redigering af logons på side 20 for at få flere oplysninger.
   - **Log ind**—Log ind på den valgte konto.
   - **Slet**—Slet logon'et for den valgte konto.

For at knytte et yderligere logon til en webside eller et program:

1. Åbn programmets eller websidens login-skærm.
2. Klik eller tryk på ikonet **Password Manager** for at vise kontekstmenuen.
3. Klik eller tryk på **Add Logon** (Tilføj logon), og følg derefter anvisningerne på skærmen.

Vurdering af din adgangskodes styrke

Det er vigtigt at bruge stærke adgangskoder til logon på websider og programmer, for at beskytte din identitet.

Password Manager gør det nemt at overvåge og forbedre din sikkerhed med øjeblikkelig og automatiseret analyse af styrken for hver enkelt af de adgangskoder, som benyttes til at logge ind på dine websider og programmer.

Mens du indtaster en adgangskode i forbindelse med oprettelse af et Password Manager-logon til en konto, viser en farvet bjælke under adgangskoden hvor stærk adgangskoden er. Farverne indikerer følgende værdier:

- **Rød**—Svag
- **Gul**—Nogenlunde
- **Green**—Stærk

Indstillinger for ikonet Password Manager

Password Manager forsøger at identificere logon-skærme til websider og programmer. Når der opdages en logon-skærm, som du ikke allerede har oprettet et logon til, beder Password Manager dig om at knytte et logon til skærmen ved at vise ikonet **Password Manager** med et plus-tegn.

1. Klik eller tryk på ikonet, og klik eller tryk derefter på **Icon Settings** (Indstillinger for ikon) for at tilpasse Password Managers håndtering af mulige logon-steder.
   - **Prompt to add logons for logon screens** (Bed om at knytte logons til logon-skærme)—Klik eller tryk på denne valgmulighed for at få Password Manager til at bede dig om at tilføje et logon, når der vises en logon-skærm, som ikke allerede har et tilknyttet logon.
   - **Exclude this screen** (Udelad denne skærm)—Vælg afkrydsningsfeltet, sådan at Password Manager ikke igen beder dig om at knytte et logon til denne logon-skærm.
   - **Do not prompt to add logons for logon screens** (Bed ikke om at tilføje logons til logon-skærme)—Vælg alternativknappen.
2. For føje et logon til en skærm som tidligere er blevet udeladt:
   a. Log ind på den webside som tidligere er blevet udeladt.
   b. For at få Password Manager til at huske adgangskoden til dette websted skal du klikke eller trykke på **Husk** i pop-up-dialogboksen for at gemme adgangskoden og oprette et login til skærmen.
3. For at få adgang til yderligere indstillinger for Password Manager, klik eller tryk på ikonet Password Manager, klik eller tryk på **Åbn Password Manager**, og klik eller tryk derefter på **Indstillinger** på siden Password Manager.

Import og eksport af logons

På siden HP Password Manager Import og Eksport, kan du importere logons, som er gemt af webbrowsere på din computer. Du kan også importere data fra en HP Client Security sikkerhedskopifil og eksportere data til en HP Client Security sikkerhedskopifil.

▲ For at åbne siden Import og eksport, klik eller tryk på **Import og eksport** på siden Password Manager.

For at importere adgangskoder fra en browser:

1. Klik eller tryk på den browser, hvorfra du ønsker at importere adgangskoder (kun installerede browsere vises).
2. Ryd afkrydsningsfelterne for alle konti, for hvilke du ikke ønsker at importere adgangskoder.
3. Klik eller tryk på **Importer**.

Import af data fra, eller eksport af data til, en HP Client Security sikkerhedskopifil kan foretages ved hjælp af de tilknyttede links (under **Other Options** (andre muligheder)) på siden Import og eksport.

BEMÆRK: Denne funktion importerer og eksporterer kun data til og fra Password Manager. For oplysninger om sikkerhedskopiering og gendannelse af andre HP Client Security-data, se Sikkerhedskopiering og gendannelse af dine data på side 27.

For at importere data fra en HP Client Security sikkerhedskopifil:

1. Fra siden HP Password Manager Import og Eksport, klik eller tryk på **Import data from an HP Client Security backup file** (Importer data fra en HP Client Security sikkerhedskopifil).
2. Bekræft din identitet.
3. Vælg den sikkerhedskopifil som tidligere er blevet oprettet, eller indtast stien i feltet, og klik eller tryk derefter på **Gennemse**.
4. Indtast den adgangskode, som benyttes til at beskytte filen, og klik eller tryk derefter på **Næste**.
5. Klik eller tryk på **Restore** (Gendan).

For at eksportere data til en HP Client Security sikkerhedskopifil:

1. Fra siden HP Password Manager Import og Eksport, klik eller tryk på **Export data from an HP Client Security backup file** (Eksporter data fra en HP Client Security sikkerhedskopifil).
2. Bekræft din identitet, og klik eller tryk derefter på **Næste**.
3. Indtast et navn til sikkerhedskopifilen. Som standard gemmes filen i mappen Dokumenter. For at angive en anden placering, klik eller tryk på **Gennemse**.
4. Indtast og bekræft en adgangskode for at beskytte filen, og klik eller tryk derefter på **Gem**.

Indstillinger

Du kan angive indstillinger til personlig tilpasning af Password Manager:

- **Prompt to add logons for logon screens** (Bed om at knytte logons til logonskærme)—Ikonet **Password Manager** vises med et plus-tegn, hver gang en logon-skærm til en webside eller et program registreres, hvilket indikerer at du kan knytte et logon for denne skærm til menuen **Logons**.

  For at deaktivere denne funktion, ryd afkrydsningsfeltet ved siden af **Prompt to add logons for logon screens** (Bed om at tilføje logons til logon-skærme).

- **Åbn Password Manager med Ctrl+Win+h**—Standard genvejstasten der åbner menuen **Password Manager hurtiglinks** er Ctrl+Windows-tasten+h.

  For at ændre genvejstasten, klik eller tryk på denne valgmulighed, og angiv derefter en ny tastkombination. Kombinationerne kan omfatte en eller flere af følgende: Ctrl, alt, eller skift og enhver alfabetisk eller numerisk tast.

  Kombinationer som er reserveret til Windows eller Windows-programmer kan ikke benyttes.

- For at nulstille indstillingerne til fabriksstandarden, klik eller tryk på **Gendan standarder**.

Avancerede indstillinger

Administratorer kan få adgang til følgende valgmuligheder ved at vælge ikonet **Gear** (Indstillinger) på HP Client Security startskærmbilledet.

- **Administrator Policies** (Administrator-politikker)—Her kan du konfigurere logon- og session-politikker for administratorer.
- **Standard User Policies** (Standardbruger-politikker)—Her kan du konfigurere logon- og session-politikker for standardbrugere.
- **Sikkerhedsfunktioner**—Her kan du forøge din computers sikkerhed ved at beskyttelse din Windows-konto med sikker godkendelse og/eller ved at aktivere godkendelse før Windows startes.
- **Brugere**—Giver dig mulighed for at styre brugere og deres legitimationsoplysninger.
- **Mine politikker**—Her kan du se dine godkendelsespolitikker og registreringsstatus.
- **Sikkerhedskopier og gendan**—Her kan du sikkerhedskopiere eller gendanne HP Client Security-data.
- **Om HP Client Security**—Viser versionsoplysninger om HP Client Security.

Administratorpolitikker

Du kan konfigurere logon- og sessionpolitikker for denne computers administratorer. Logon-politikker som indstilles her, styrer de legitimationsoplysninger, som kræves for at en lokal administrator kan logge på Windows. Session-politikker som indstilles her, styrer de legitimationsoplysninger, som kræves for at en lokal administrator kan bekræfte sin identitet inden for en Windows-session.

Som standard træder alle nye og ændrede politikker i kraft med det samme, når der klikkes eller trykkes på **Anvend**.

For at tilføje en ny politik:

1. På HP Client Security startsiden, klik eller tryk på ikonet **Gear** (indstillinger).
2. På siden Avancerede indstillinger, klik eller tryk på **Administratorpolitikker**.
3. Klik eller tryk på **Tilføj ny politik**.
4. Klik på pil ned for at vælge primære og (eventuelle) sekundære legitimationsoplysninger for den nye politik, og klik eller tryk derefter på **Tilføj**.
5. Klik på **Apply** (Anvend).

For at forsinke en ny eller ændret politiks ikrafttræden:

1. Klik eller tryk på **Enforce this policy immediately** (Anvend denne politik med det samme).
2. Vælg **Enforce this policy on the specific date** (Anvend denne politik på en specifik dato).
3. Indtast en dato eller benyt pop-op kalenderen til at vælge den dato hvor politikken skal træde i kraft.
4. Hvis det ønskes, kan der også vælges et tidspunkt, hvor brugere mindes om den nye politik.
5. Klik på **Apply** (Anvend).

Standardbrugerpolitikker

Du kan konfigurere logon- og sessionpolitikker for denne computers standardbrugere. Logon-politikker som indstilles her, styrer de legitimationsoplysninger, som kræves for at en standardbruger kan logge på Windows. Session-politikker som indstilles her, styrer de legitimationsoplysninger, som kræves for at en standardbruger kan bekræfte sin identitet inden for en Windows-session.

Som standard træder alle nye og ændrede politikker i kraft med det samme, når der klikkes eller trykkes på **Anvend**.

For at tilføje en ny politik:

1. På HP Client Security startsiden, klik eller tryk på ikonet **Gear** (indstillinger).
2. På siden Avancerede indstillinger, klik eller tryk på **Standardbrugerpolitikker**.
3. Klik eller tryk på **Tilføj ny politik**.
4. Klik på pil ned for at vælge primære og (eventuelle) sekundære legitimationsoplysninger for den nye politik, og klik eller tryk derefter på **Tilføj**.
5. Klik på **Apply** (Anvend).

For at forsinke en ny eller ændret politiks ikrafttræden:

1. Klik eller tryk på **Enforce this policy immediately** (Anvend denne politik med det samme).
2. Vælg **Enforce this policy on the specific date** (Anvend denne politik på en specifik dato).
3. Indtast en dato eller benyt pop-op kalenderen til at vælge den dato hvor politikken skal træde i kraft.
4. Hvis det ønskes, kan der også vælges et tidspunkt, hvor brugere mindes om den nye politik.
5. Klik på **Apply** (Anvend).

Sikkerhedsfunktioner

Du kan aktivere funktioner i HP Client Security, som hjælper til at beskytte mod uautoriseret adgang til computeren.

For at opsætte sikkerhedsfunktioner:

1. På HP Client Security startsiden, klik eller tryk på ikonet **Gear** (indstillinger).
2. På siden Avancerede indstillinger, klik eller tryk på **Sikkerhedsfunktioner**.
3. Aktiver sikkerhedsfunktioner ved at vælge afkrydsningsfelterne og derefter klikke eller trykke på **Anvend**. Jo flere funktioner du vælger, jo mere sikker er din computer.

   Disse indstillinger gælder for alle brugere.

   - **Windows logon-sikkerhed**—Beskytter dine Windows-konti ved at kræve HP Client legitimationsoplysninger til sikkerhed ved adgang.
   - **Før start-sikkerhed (opstartsgodkendelse)**—Beskytter din computer før Windows starter. Denne valgmulighed er ikke tilgængelig, hvis systemets BIOS ikke understøtter det.
   - **Allow One Step logon** (Tillad logon et-trins logon)—Denne indstilling springer over Windows logon, hvis der tidligere er blevet foretaget godkendelse med opstartsgodkendelse eller via Drive Encryption.
4. Klik eller tryk på **brugere** og klik eller tryk derefter på brugerens flise.

Brugere

Du kan overvåge og administrere denne computers HP Client Security-brugere.

For at føje en Windows-bruger til HP Client Security:

1. På HP Client Security startsiden, klik eller tryk på ikonet **Gear** (indstillinger).
2. På siden Avancerede indstillinger, klik eller tryk på **Brugere**.
3. Klik eller tryk på **Add another Windows user to HP Client Security** (Føj en Windows-bruger til HP Client Security).
4. Indtast navnet på den bruger du ønsker at tilføje, og klik eller tryk derefter på **OK**.
5. Indtast brugerens adgangskode til Windows.

   Et felt for den tilføjede bruger vises på siden Bruger.

For at slette en Windows-bruger fra HP Client Security:

1. På HP Client Security startsiden, klik eller tryk på ikonet **Gear** (indstillinger).
2. På siden Avancerede indstillinger, klik eller tryk på **Brugere**.
3. Klik eller tryk på navnet på den bruger du ønsker at slette.
4. Klik eller tryk på **Slet bruger** og klik eller tryk derefter på **Ja** for at bekræfte.

For at vise en oversigt over logon- og sessionpolitikker, der gælder for en bruger:

▲ Klik eller tryk på **brugere** og klik eller tryk derefter på brugerens flise.

My Policies (Mine politikker)

Du kan få vist dine godkendelsespolitikker og registreringsstatus. Siden My Policies (Mine politikker) indeholder også links til administratorpolitikker og standardbrugerpolitikker.

1. På HP Client Security startsiden, klik eller tryk på ikonet **Gear** (indstillinger).
2. På siden Avancerede indstillinger, klik eller tryk på **My Policies** (Mine politikker).

   De logon- og sessionpolitikker der gælder for de brugere der for øjeblikket er logget på, vises.

Siden My Policies (Mine politikker) indeholder også links til Administratorpolitikker på side 25 og Standardbrugerpolitikker på side 26.

Sikkerhedskopiering og gendannelse af dine data

Det anbefales at du regelmæssigt sikkerhedskopierer dine HP Client Security data. Hyppigheden af sikkerhedskopieringen afhænger af, hvor ofte disse data ændres. Hvis du for eksempel dagligt tilføjer nye logons, bør du også foretage sikkerhedskopiering på daglig basis.

Sikkerhedskopier kan også benyttes til at migrere fra en computer til en anden, hvilket også kaldes import og eksport.

BEMÆRK: Det er kun Password Manager, der sikkerhedskopieres med denne funktion. Drive Encryption har en uafhængig metode til sikkerhedskopiering. Device Access Manager og informationer til fingeraftryksgodkendelse sikkerhedskopieres ikke.

Hvis data skal gendannes fra en sikkerhedskopifil, skal HP Client Security først være installeret på den computer, som skal modtage de sikkerhedskopierede data.

Sådan sikkerhedskopieres dine data:

1. På HP Client Security startsiden, klik eller tryk på ikonet **Gear** (indstillinger).
2. På siden Avancerede indstillinger, klik eller tryk på **Administratorpolitikker**.
3. Klik eller tryk på **Sikkerhedskopiering og gendannelse**.
4. Klik eller tryk på **Sikkerhedskopier**, og bekræft derefter din identitet.
5. Vælg det modul, som du ønsker at medtage i sikkerhedskopien, og klik eller tryk derefter på **Næste**.
6. Indtast et navn til lagerfilen. Som standard gemmes filen i mappen Dokumenter. For at angive en anden placering, klik eller tryk på **Gennemse**.
7. Indtast og bekræft en adgangskode for at beskytte filen.
8. Klik eller tryk på **Gem**.

Sådan gendannes dine data:

1. På HP Client Security startsiden, klik eller tryk på ikonet **Gear** (indstillinger).
2. På siden Avancerede indstillinger, klik eller tryk på **Administratorpolitikker**.
3. Klik eller tryk på **Sikkerhedskopiering og gendannelse**.
4. Vælg **Gendan**, og bekræft derefter din identitet.
5. Vælg den lagerfil du oprettede tidligere. Indtast stien i det dertil indrettede felt. For at angive en anden placering, klik eller tryk på **Gennemse**.
6. Indtast den adgangskode, som benyttes til at beskytte filen, og klik eller tryk derefter på **Næste**.
7. Vælg de moduler, som du ønsker at gendanne data for.
8. Klik eller tryk på **Restore** (Gendan).

5 HP Drive Encryption (kun udvalgte modeller)

HP Drive Encryption giver fuldstændig databeskyttelse ved at kryptere din computers data. Når Drive Encryption aktiveres, skal du logge ind på Drive Encryptions logonskærmbillede, der vises, før Windows®-operativsystemet starter.

HP Client Security startskærmen gør det muligt for Windows-administratorer at aktivere Drive Encryption, sikkerhedskopiere krypteringsnøglen, og vælge eller fravælge drev eller partition(er) som skal krypteres. Yderligere oplysninger finder du i hjælpen til HP Client Security software.

Følgende opgaver kan udføres med Drive Encryption:

- Valg af indstillinger for Drive Encryption:
  - Kryptering eller dekryptering af individuelle drev eller partitioner via software-kryptering
  - Kryptering eller dekryptering af individuelle selvkrypterende drev via hardware-kryptering
  - Tilføjelse af yderligere sikkerhed ved at deaktivere slumre- eller standby-tilstand, for at sikre at Drive Encryption før start-godkendelse altid er påkrævet

BEMÆRK: Kun interne SATA- og eksterne eSATA-harddiske kan krypteres.

- Oprettelse af sikkerhedskopier af nøgler
- Genskabelse af adgang til en krypteret computer ved hjælp af sikkerhedskopierede nøgler og HP SpareKey
- Aktivering af Drive Encryption før start-godkendelse ved hjælp af adgangskode, registreret fingeraftryk eller PIN-kode for udvalgte chipkort

Åbning af Drive Encryption

Administrator kan få adgang til Drive Encryption ved at åbne HP Client Security:

1. Fra startskærmen klikkes eller trykkes på appen **HP Client Security** (Windows 8).

   - eller -

   Fra Windows-skrivebordet, dobbeltklik eller dobbelttryk på ikonet **HP Client Security** i meddelelsesområdet, som er placeret længst til højre på proceslinjen.

2. Klik eller tryk på ikonet **Drive Encryption**.

Generelle opgaver

Aktivering af Drive Encryption for standard-harddiske

Standard-harddiske krypteres ved hjælp af software-kryptering. Følg disse trin for at kryptere et drev eller en diskpartition:

1. Start **Drive Encryption**. Se Åbning af Drive Encryption på side 29 for at få flere oplysninger.
2. Vælg afkrydsningsfeltet for det drev eller den partition som skal krypteres, og klik eller tryk derefter på **Backup Key** (Sikkerhedskopier nøgle).

BEMÆRK: For yderligere sikkerhed, vælg afkrydsningsfeltet **Disable sleep mode for increased security** (Deaktiver slumretilstand for yderligere sikkerhed). Når du deaktiverer slumretilstand, er der absolut ingen risiko for at de legitimationsoplysninger, som bruges til at låse op for drevene, lagres i hukommelsen.

3. Vælg en eller flere af valgmulighederne for sikkerhedskopiering, og klik eller tryk på **Sikkerhedskopier**. Se Sikkerhedskopiering af krypteringsnøgler på side 33 for at få flere oplysninger.
4. Du kan fortsætte med at arbejde mens krypteringsnøglen sikkerhedskopieres. Genstart ikke computeren.

BEMÆRK: Du bliver senere bedt om at genstarte computeren. Efter genstarten vises skærmen Drive Encryption pre-boot (før start), som kræver godkendelse før Windows kan startes.

Drive Encryption er blevet aktiveret. Kryptering af den/de valgte drev-partition(er) kan tage flere timer, alt afhængig antallet og størrelsen af partitionen/partitionerne.

Yderligere oplysninger finder du i hjælpen til HP Client Security software.

Sådan aktiveres Drive Encryption på selvkrypterende drev

Selvkrypterende drev, som overholder Trusted Computing Group's OPAL-specifikationer for administration af selvkrypterende drev, kan krypteres med enten software-kryptering eller hardware-kryptering. Hardware-kryptering er langt hurtigere end software-kryptering. Man kan til gengæld ikke vælge hvilke diskpartitioner der skal krypteres. Hele disken, inklusive eventuelle partitioner, krypteres.

For at kryptere specifikke partitioner, skal du vælge software-kryptering. Sørg for at rydde afkrydsningsfeltet **Only allow hardware encryption for Self-Encrypting Drives (SEDs)** (Tillad kun hardware-kryptering for selvkrypterende drev (SED'er).

Følg disse trin for at aktivere Drive Encryption på selvkrypterende drev:

1. Start **Drive Encryption**. Se Åbning af Drive Encryption på side 29 for at få flere oplysninger.
2. Vælg afkrydsningsfeltet for det drev som skal krypteres, og klik eller tryk derefter på **Backup Key** (Sikkerhedskopier nøgle).

BEMÆRK: For yderligere sikkerhed, vælg afkrydsningsfeltet **Disable sleep mode for added security** (Deaktiver slumretilstand for yderligere sikkerhed). Når du deaktiverer slumretilstand, er der absolut ingen risiko for at de legitimationsoplysninger, som bruges til at låse op for drevene, lagres i hukommelsen.

3. Vælg en eller flere af valgmulighederne for sikkerhedskopiering, og klik eller tryk på **Sikkerhedskopier**. Se Sikkerhedskopiering af krypteringsnøgler på side 33 for at få flere oplysninger.
4. Du kan fortsætte med at arbejde mens krypteringsnøglen sikkerhedskopieres. Genstart ikke computeren.

BEMÆRK: Ved selvkrypterende drev bliver du bedt om at lukke computeren.

Yderligere oplysninger finder du i hjælpen til HP Client Security software.

Deaktivering af Drive Encryption

1. Start **Drive Encryption**. Se Åbning af Drive Encryption på side 29 for at få flere oplysninger.
2. Ryd afkrydsningsfeltet for alle krypterede drev, og klik eller tryk derefter på **Anvend**.

   Deaktivering af Drive Encryption starter.

BEMÆRK: Hvis der blev benyttet software-kryptering, starter dekryptering. Det kan tage flere timer, alt afhængig størrelsen af den/de krypterede partition/partitioner. Når dekrypteringen er gennemført, deaktiveres Drive Encryption.

Hvis der blev benyttet hardware-kryptering, dekrypteres drevet med det samme og Drive Encryption deaktiveres efter nogle få minutter.

Når Drive Encryption er deaktiveret, vil du blive bedt om at lukke computeren, hvis du benyttede hardware-kryptering, eller genstarte computeren, hvis du benyttede software-kryptering.

Indlogning efter aktivering af Drive Encryption

Når du tænder for computeren efter aktivering af Drive Encryption, skal du logge ind via Drive Encryption login-skærmen:

BEMÆRK: Når computeren vækkes fra slumre- eller standby-tilstand, vises Drive Encryption før start-godkendelse ikke, hverken ved software- eller hardware-kryptering. Hardware-kryptering har valgmuligheden **Disable sleep mode for increased security** (Deaktiver slumretilstand for at øge sikkerheden), som, når den er aktiveret, forhindrer computeren i at gå i slumre- eller standby-tilstand .

Når computeren vækkes fra dvale vises Drive Encryption før start-godkendelse for både software- og hardware-kryptering.

BEMÆRK: Hvis Windows-administratoren har aktiveret BIOS før start-sikkerhed i HP Client Security og hvis One-Step Logon er aktiveret (som standard), kan du logge ind på computeren med det samme efter at have opnået godkendelse ved BIOS før-start, uden at skulle opnå godkendelse igen ved Drive Encryption login-skærmen.

Logon for enkelt bruger:

- ▲ Indtast din Windows-adgangskode, PIN-kode til chipkort, SpareKey eller stryg en registreret finger på **Logon**-siden.

Logon for flere brugere:

1. Vælg den bruger der skal logges ind fra rullelisten på siden **Select user to logon** (Vælg den bruger der skal logges på), og klik eller tryk derefter på **Næste**.
2. Indtast din Windows-adgangskode, PIN-kode til chipkort eller stryg en registreret finger på **Logon**-siden.

BEMÆRK: Følgende chipkort understøttes:

Understøttede chipkort

- Gemalto Cyberflex Access 64k V2c

BEMÆRK: Hvis gendannelsesnøglen bruges til at logge ind på Drive Encryption login-skærmen, kræves der yderligere legitimationsoplysninger ved Windows logon for at få adgang til brugerkonti.

Kryptering af yderligere harddiske

Det anbefales på det kraftigste at man benytter HP Drive Encryption til at beskytte data ved at kryptere harddisken. Efter aktivering kan tilføjede harddiske eller partitioner krypteres ved at følge disse trin:

1. Start **Drive Encryption**. Se Åbning af Drive Encryption på side 29 for at få flere oplysninger.
2. For software-krypterede drev, vælg de partitioner som skal krypteres.

BEMÆRK: Dette gælder også for situationer med forskellige drev, hvor der er en eller flere standard-harddiske og et eller flere selvkrypterende drev.

- eller -

▲ For hardware-krypterede drev, vælg det eller de yderligere drev, som skal krypteres.

Avancerede opgaver

Administration af Drive Encryption (administrator-opgave)

Administratorer kan benytte Drive Encryption til at se og ændre status for kryptering (Ikke krypteret eller krypteret) på alle computerens harddiske.

- Hvis status er Aktiveret, betyder det at Drive Encryption er blevet aktiveret og konfigureret. Drevet er i en af følgende tilstande:

Software-kryptering

- Ikke krypteret
- Krypteret
- Krypterer
- Dekrypterer

Hardware-kryptering

- Krypteret
- Ikke krypteret (for ekstra drev)

Kryptering eller dekryptering af individuelle drev-partitioner (kun ved softwarekryptering)

Administratorer kan benytte Drive Encryption til at kryptere en eller flere harddisk-partition(er) på computeren eller dekryptere drev-partition(er) som allerede er blevet krypteret.

1. Start **Drive Encryption**. Se Åbning af Drive Encryption på side 29 for at få flere oplysninger.
2. Vælg eller ryd afkrydsningsfeltet ved siden af hver af de harddisk-partitioner som skal krypteres eller dekrypteres under **Drive Status** (Drevstatus) og klik eller tryk derefter på **Anvend**.

BEMÆRK: Når en partition krypteres eller dekrypteres, viser en statuslinje hvor mange procent af partitionen, der er krypteret.

BEMÆRK: Dynamiske partitioner understøttes ikke. Hvis en partition vises som tilgængelig, men ikke kan krypteres når den vælges, er det fordi den er dynamisk. En dynamisk partition opstår når en partition formindskes for at oprette en ny partition med Diskhåndtering.

En advarsel vises, hvis en partition konverteres til en dynamisk partition.

Diskhåndtering

- **Kaldenavn**—Du kan give dine drev eller partitioner navne, for at gøre det nemmere at identificere dem.
- **Drev som ikke er tilsluttet**—Drive Encryption kan følge diske som fjernes fra computeren. En disk som fjernes fra computeren flyttes automatisk til listen Disconnected (Ikke tilsluttet). Hvis disken tilsluttes systemet igen, bliver den automatisk flyttet tilbage til listen Connected (Tilsluttet).
- Hvis du ikke længere har brug for at følge eller administrere et drev, som ikke er tilsluttet, kan du fjerne de fra listen Disconnected (Ikke tilsluttet).
- Drive Encryption vil fortsat være aktiveret, indtil afkrydsningsfelterne for alle tilsluttede drev er ryddet, og listen Disconnected (Ikke tilsluttet) er tom.

Sikkerhedskopiering og gendannelse (administrator-opgave)

Når Drive Encryption er aktiveret, kan administratorer bruge siden Encryption Key Backup (Sikkerhedskopiering af krypteringsnøgle) til at sikkerhedskopiere krypteringsnøgler til flytbare medier og til at udføre en gendannelse.

Sikkerhedskopiering af krypteringsnøgler

Administratorer kan sikkerhedskopiere et krypteret drevs krypteringsnøgle til en flytbar lagerenhed.

FORSIGTIG: Sørg for at opbevare den lagerenhed, som indeholder sikkerhedskopien af nøglen, på et sikkert sted, for hvis du glemmer din adgangskode, mister dit chipkort, eller ikke har en finger registreret, er det kun denne enhed der kan give dig adgang til computeren. Opbevaringsstedet skal også være sikkert, for lagerenheden giver adgang til Windows.

1. Start **Drive Encryption**. Se Åbning af Drive Encryption på side 29 for at få flere oplysninger.
2. Vælg afkrydsningsfeltet for et drev, og klik eller tryk derefter på **Backup Key** (Sikkerhedskopier nøgle).

3. Vælg en eller flere af nedenstående muligheder under **Create HP Drive Encryption recovery key** (Opret HP Drive Encryption gendannelsesnøgle):

   - **Removable Storage** (Flytbart lager)—Vælg afkrydsningsfeltet, og vælg derefter den lagerenhed hvor krypteringsnøglen skal gemmes.
   - **SkyDrive**—Vælg afkrydsningsfeltet. Du skal være forbundet til internettet. Log ind på Microsoft SkyDrive, og klik eller tryk derefter på **Ja**.

   BEMÆRK: For at bruge den sikkerhedskopierede HP Drive Encryption-nøgle, som er gemt på SkyDrive, skal du downloade den fra SkyDrive til en flytbar lagerenhed, og derefter slutte lagerenheden til denne computer.

   - **TPM** (kun udvalgte modeller)—Gør det muligt at gendanne dine data ved hjælp af din TPM-adgangskode.

   FORSIGTIG: Hvis TPM'en slettes eller computeren bliver skadet, vil du miste adgangen til sikkerhedskopien. Hvis denne metode er valgt, bør en anden sikkerhedskopieringsmetode også vælges.

4. Klik eller tryk på **Sikkerhedskopier**.

   Krypteringsnøglen gemmes på den lagerenhed du har valgt.

Gendannelse af adgang til en aktiveret computer ved hjælp af sikkerhedskopier af nøgler

Administratorer kan udføre en gendannelse ved hjælp af den Drive Encryption-nøgle, som er blevet sikkerhedskopieret til en flytbar lagerenhed ved aktivering eller ved at vælge muligheden **Backup Key** (sikkerhedskopi af nøgle) i Drive Encryption.

1. Tilslut den flytbare lagerenhed, som indeholder sikkerhedskopien af nøglen.
2. Tænd for computeren.
3. Når login-dialogboksen til HP Drive Encryption åbnes, skal du klikke eller trykke på **Recovery** (Gendannelse).
4. Indtast den sti eller det navn, som indeholder sikkerhedskopien af nøglen, og klik eller tryk derefter på **Recovery** (Gendannelse).
5. Når bekræftelsesdialogboksen åbnes, klik eller tryk på **OK**.

   Windows logon-skærmen vises.

BEMÆRK: Hvis gendannelsesnøglen bruges til at logge på ved Drive Encryption login-skærmen, kræves der yderligere legitimationsoplysninger ved Windows logon for at få adgang til brugerkonti. Det anbefales på det kraftigste at du nulstiller din adgangskode efter at have gennemført en gendannelse.

Udførelse af en HP SpareKey gendannelse

SpareKey gendannelse inden for Drive Encryption før-start kræver at du svarer korrekt på sikkerhedsspørgsmålene, før du kan få adgang til computeren. For flere oplysninger om SpareKey gendannelse, se software-hjælpen til HP Client Security.

For at gennemføre en gendannelse med HP SpareKey Recovery, hvis du har glemt din adgangskode:

1. Tænd for computeren.
2. Når HP Drive Encryption-siden vises, skal du navigere til bruger login-siden.

3. Klik på **SpareKey**.

BEMÆRK: Hvis din SpareKey ikke er blevet initialiseret i HP Client Security, vises knappen **SpareKey** ikke.

4. Indtast korrekt svar på det valgte spørgsmål, og klik derefter på **Login**.

   Windows logon-skærmen vises.

BEMÆRK: Hvis SpareKey bruges til at logge ind på Drive Encryption login-skærmen, kræves der yderligere legitimationsoplysninger ved Windows logon for at få adgang til brugerkonti. Det anbefales på det kraftigste at du nulstiller din adgangskode efter at have gennemført en gendannelse.

6 HP File Sanitizer (kun udvalgte modeller)

File Sanitizer muliggør sikker makulering af aktiver (f.eks.: Personlige oplysninger eller filer, historiske eller webrelaterede data eller andre datakomponenter) på computerens interne harddisk og jævnligt at overskrive computerens interne harddisk.

File Sanitizer kan ikke bruges til at rense eller overskrive drev af følgende typer:

- SSD-drev (solid-state drive), deriblandt RAID-diskenheder som omfatter en SSD-enhed
- Eksterne drev, som er tilsluttet via USB, Firewire, eller eSATA-grænseflade

Hvis en makulerings- eller overskrivelses-handling forsøges på et SSD-drev, vises en advarselsmeddelelse, og handlingen gennemføres ikke.

Makulering

Makulering adskiller sig fra en normal Windows®-sletning. Når du makulerer et aktiv med File Sanitizer, overskrives filerne med tilfældige data, hvilket gør det stort set umuligt at genskabe det oprindelige aktiv. En almindelig Windows-sletning efterlader muligvis filen (eller aktivet) intakt på harddisken eller i en tilstand hvor tekniske metoder kan benyttes til at genskabe filen eller aktivet.

Du kan planlægge et fremtidigt tidspunkt for makulering, eller du kan manuelt aktivere makulering ved at vælge ikonet **File Sanitizer** på HP Client Security Home-skærmen eller via **File Sanitizer** ikonet på Windows-skrivebordet. For flere oplysninger, se Indstilling af en plan for makulering på side 38, Makulering med højreklik på side 40, eller Manuel start af makulering på side 40.

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

Overskrivning af ledig plads

Hvis man sletter et aktiv i Windows, fjernes aktivets indhold ikke fuldstændigt fra harddisken. Windows sletter kun referencen til aktivet, eller dets placering på harddisken. Aktivets indhold findes stadig på harddisken, indtil et andet aktiv overskriver det samme område på harddisken med ny information.

Overskrivning af ledig plads gør det muligt at skrive tilfældige data sikkert over slettede aktiver, hvilket forhindrer brugere i at se aktivets oprindelige indhold.

BEMÆRK: Overskrivning af ledig plads giver ingen yderligere sikkerhed til makulerede aktiver.

Du kan indstille et fremtidigt tidspunkt for overskrivning af ledig plads, eller du kan manuelt aktivere overskrivning af aktiver, som tidligere er blevet makuleret, ved at vælge ikonet **File Sanitizer** på HP Client Security Home-skærmen eller via **File Sanitizer** ikonet på Windows-skrivebordet. For flere oplysninger, se Indstilling af plan for overskrivning af ledig plads på side 39, Manuel start af overskrivning af ledig plads på side 41, eller Sådan bruges ikonet File Sanitizer på side 40.

Sådan åbnes File Sanitizer

1. Fra startskærmen klikkes eller trykkes på appen **HP Client Security** (Windows 8).

   - eller -

   Fra Windows-skrivebordet, dobbeltklik eller dobbelttryk på ikonet **HP Client Security** i meddelelsesområdet, som er placeret længst til højre på proceslinjen.

2. Under **Data**, klik eller tryk på **File Sanitizer**.

- eller -

▲ Dobbeltklik eller dobbelttryk på ikonet **File Sanitizer** på Windows-skrivebordet.

- eller -

▲ Højreklik på ikonet **File Sanitizer** på Windows-skrivebordet eller tryk på det og hold det nede, og vælg derefter **Åbn File Sanitizer**.

Opsætningsprocedurer

Makulering—File Sanitizer sletter eller makulerer udvalgte kategorier af aktiver på sikker vis.

1. Vælg afkrydsningsfeltet for hver af de typer af filer som skal makuleres under **Makulering**, eller ryd afkrydsningsfeltet hvis du ikke ønsker at makulere disse filer.

   - **Papirkurv**—Makulerer alle elementer i papirkurven.
   - **Midlertidige systemfiler**—Makulerer alle filer i systemets midlertidige mappe. De følgende miljøvariabler gennemsøges i følgende rækkefølge, og den første sti der bliver fundet, regnes for at være systemmappen:
     - TMP
     - TEMP
   - **Midlertidige internetfiler**—Makulerer kopier af websider, billeder og medier, som gemmes af webbrowsere med henblik på hurtigere visning.
   - **Cookies**—Makulerer alle filer, som gemmes på computeren af websteder, for at gemme indstillinger, såsom login-oplysninger.

2. For at påbegynde makuleringen, klik eller tryk på **Makuler**.

Overskrivning—Skriver tilfældige data til ledig plads og forhindrer gendannelse af slettede elementer.

▲ For at påbegynde overskrivning, klik eller tryk på **Overskriv**.

File Sanitizer Indstillinger—Vælg afkrydsningsfeltet for at aktivere hver af følgende valgmuligheder, eller ryd afkrydsningsfeltet for at deaktivere en valgmulighed:

- **Aktiver skrivebordsikon**—Viser File Sanitizer-ikonet på Windows-skrivebordet.
- **Aktiver højreklik**—Gør det muligt at højreklikke eller trykke og holde nede på et aktiv, og derefter vælge **HP File Sanitizer – Makuler**.

- **Ask for Windows password before manual shredding** (Bed om Windows adgangskode før makulering)—Kræver godkendelse med Windows-adgangskode før manuel makulering af et element.
- **Shred Cookies og Temporary Internet Files on browser close** (Makuler cookies og midlertidige internetfiler når browser lukkes—Makulerer alle udvalgte web-relaterede aktiver, såsom browserens URL-historie, når du lukker en webbrowser.

Indstilling af en plan for makulering

Du kan planlægge et tidspunkt, hvor makulering automatisk skal udføres, eller du kan til enhver tid makulere aktiver manuelt. Yderligere oplysninger finder du i Opsætningsprocedurer på side 37.

1. Åbn File Sanitizer, og klik eller tryk derefter på **Indstillinger**.
2. For at planlægge en fremtidig makulering, kan man under **Shred Schedule** (Makuleringsplan) vælge **Aldrig**, **Én gang**, **Dagligt**, **Ugentligt**, eller **Månedligt**, og derefter vælge en dag og et tidspunkt:
   a. Klik eller tryk på feltet for time, minut eller AM/PM.
   b. Rul indtil den ønskede værdi vises på samme niveau som de andre felter.
   c. Klik eller tryk på det hvide område, som omgiver tidsindstillingsfelterne.
   d. Gentag for hvert felt, indtil den korrekte plan er blevet valgt.
3. Følgende fire typer af aktiver er medtaget på listen:
   - **Papirkurv**—Makulerer alle elementer i papirkurven.
   - **Midlertidige systemfiler**—Makulerer alle filer i systemets midlertidige mappe. De følgende miljøvariabler gennemsøges i følgende rækkefølge, og den første sti der bliver fundet, regnes for at være systemmappen:
     - TMP
     - TEMP
   - **Midlertidige internetfiler**—Makulerer kopier af websider, billeder og medier, som gemmes af webbrowsere med henblik på hurtigere visning.
   - **Cookies**—Makulerer alle filer, som gemmes på computeren af websteder, for at gemme indstillinger, såsom login-oplysninger.

   Hvis de vælges, makuleres disse aktiver på det planlagte tidspunkt.
4. For at foretage yderligere tilpassede valg af aktiver:
   a. Under **Scheduled Shred List** (Liste over planlagte makuleringer), klik eller tryk på **Tilføj mappe**, og naviger derefter til filen eller mappen.
   b. Klik eller tryk på **Åbn**, og klik eller tryk derefter på **OK**.

   For at fjerne et aktiv fra listen over planlagte makuleringer, skal man rydde aktivets afkrydsningsfelt.

Indstilling af plan for overskrivning af ledig plads

Overskrivning af ledig plads giver ingen yderligere sikkerhed til makulerede aktiver.

1. Åbn File Sanitizer, og klik eller tryk derefter på **Indstillinger**.
2. For at planlægge en fremtidig overskrivning, kan man under **Bleach Schedule** (Overskrivningsplan), vælge **Aldrig**, **Én gang**, **Dagligt**, **Ugentligt** eller **Månedligt** og derefter vælge en dag og et tidspunkt.
   a. Klik eller tryk på feltet for time, minut eller AM/PM.
   b. Rul indtil den ønskede tid vises på samme niveau som de andre felter.
   c. Klik eller tryk på det hvide område, som omgiver tidsindstillingsfelterne.
   d. Gentag, indtil den korrekte plan er blevet valgt.

BEMÆRK: Overskrivning af ledig plads kan tage forholdsvist lang tid. Sørg for at din computer er sluttet til vekselstrøm. Selv om overskrivning af ledig plads foretages i baggrunden, kan forøget brug af processoren påvirke computerens ydeevne. Overskrivning af ledig plads kan foretages efter arbejdstid eller når computeren ikke er i brug.

Sådan beskyttes filer mod makulering

For at beskytte filer eller mapper mod makulering:

1. Åbn File Sanitizer, og klik eller tryk derefter på **Indstillinger**.
2. Under **Never Shred List** (Listen makuler aldrig), klik eller tryk på **Tilføj mappe**, og naviger derefter til filen eller mappen.
3. Klik eller tryk på **Åbn**, og klik eller tryk derefter på **OK**.

BEMÆRK: Filer på denne liste beskyttes, så længe de står på listen.

For at fjerne et aktiv fra udeladelseslisten, skal man rydde afkrydsningsfeltet for aktivet.

Generelle opgaver

Brug File Sanitizer til at udføre følgende opgaver:

- **Brug ikonet File Sanitizer til at indlede makulering**—Træk filer til ikonet **File Sanitizer** på Windows-skrivebordet. For detaljer, se Sådan bruges ikonet File Sanitizer på side 40.
- **Makuler et specifikt aktiv eller alle valgte aktiver**—Makuler elementer når som helst uden at vente på en planlagt makulering. For detaljer, se Makulering med højreklik på side 40 eller Manuel start af makulering på side 40.
- **Aktiver overskrivning af ledig plads manuelt**—Aktiver overskrivning af ledig plads når som helst. For detaljer, se Manuel start af overskrivning af ledig plads på side 41.
- **Se logfilerne**—Se logfiler for makulering og overskrivning af ledig plads, som opregner fejl eller problemer i forbindelse med den seneste makulering eller overskrivning af ledig plads. For detaljer, se Visning af logfilerne på side 41.

BEMÆRK: Makulering eller overskrivning af ledig plads kan tage forholdsvist lang tid. Selv om makulering og overskrivning af ledig plads foretages i baggrunden, kan forøget brug af processoren påvirke computerens ydeevne.

Sådan bruges ikonet File Sanitizer

⚠ **FORSIGTIG:** Makulerede aktiver kan ikke gendannes. Overvej omhyggeligt hvilke elementer der skal udvælges til manuel makulering.

Når du starter en makulering manuelt, makuleres standard-makulerings-listen i File Sanitizer-visningen (se Opsætningsprocedurer på side 37).

Du kan starte en makulering manuelt på en af følgende måder:

1. Åbn File Sanitizer (se Sådan åbnes File Sanitizer på side 37), og klik eller tryk derefter på **Makuler**.
2. Når bekræftelsesdialogboksen åbnes, skal du sørge for at de aktiver som skal makuleres er markeret, og derefter klikke eller trykke på **OK**.

- eller -

1. Højreklik på ikonet **File Sanitizer** på Windows-skrivebordet eller tryk på det og hold det nede, og klik eller tryk derefter på **Makuler nu**.
2. Når bekræftelsesdialogboksen åbnes, skal du sørge for at de aktiver som skal makuleres er markeret, og derefter klikke eller trykke på **Makuler**.

Makulering med højreklik

⚠ **FORSIGTIG:** Makulerede aktiver kan ikke gendannes. Overvej omhyggeligt hvilke elementer der skal udvælges til manuel makulering.

Hvis **Enable right-click shredding** (Aktiver makulering med højreklik) er blevet aktiveret i File Sanitizer-visningen, kan du makulere et aktiv ved at gøre som følger:

1. Naviger til det dokument eller den mappe, som skal makuleres.
2. Højreklik eller tryk på og hold nede på filen eller mappen, og vælg derefter **HP File Sanitizer – Makuler**.

Manuel start af makulering

⚠ **FORSIGTIG:** Makulerede aktiver kan ikke gendannes. Overvej omhyggeligt hvilke elementer der skal udvælges til manuel makulering.

Når du starter en makulering manuelt, makuleres standard-makulerings-listen i File Sanitizer-visningen (se Opsætningsprocedurer på side 37).

Du kan starte en makulering manuelt på en af følgende måder:

1. Åbn File Sanitizer (se Sådan åbnes File Sanitizer på side 37), og klik eller tryk derefter på **Makuler**.
2. Når bekræftelsesdialogboksen åbnes, skal du sørge for at de aktiver som skal makuleres er markeret, og derefter klikke eller trykke på **OK**.

- eller -

1. Højreklik på ikonet **File Sanitizer** på Windows-skrivebordet eller tryk på det og hold det nede, og klik eller tryk derefter på **Makuler nu**.
2. Når bekræftelsesdialogboksen åbnes, skal du sørge for at de aktiver som skal makuleres er markeret, og derefter klikke eller trykke på **Makuler**.

Manuel start af overskrivning af ledig plads

Når du starter en overskrivning manuelt, overskrives standard-makulerings-listen i File Sanitizer-visningen (se Opsætningsprocedurer på side 37).

Du kan starte en overskrivning manuelt på en af følgende måder:

1. Åbn File Sanitizer (se Sådan åbnes File Sanitizer på side 37), og klik eller tryk derefter på **Overskriv**.
2. Når bekræftelsesdialogboksen åbnes, klik eller tryk på **OK**.

- eller -

1. Højreklik på ikonet **File Sanitizer** på Windows-skrivebordet eller tryk på det og hold det nede, og klik eller tryk derefter på **Overskriv nu**.
2. Når bekræftelsesdialogboksen åbnes, klik eller tryk på **Overskriv**.

Visning af logfilerne

Hver gang en makulering eller overskrivning af ledig plads gennemføres, oprettes der logfiler med eventuelle fejl eller problemer. Logfilerne opdateres altid med oplysningerne fra den seneste makulering eller overskrivning af ledig plads.

BEMÆRK: Filer som blev makuleret eller overskrevet uden problemer vises ikke i logfilerne.

Der oprettes en logfil for makuleringer, og en anden logfil for overskrivning af ledig plads. Begge logfiler er placeret på harddisken i de følgende mapper:

- C:\Programmer\Hewlett-Packard\File Sanitizer*[Brugernavn]*_ShredderLog.txt
- C:\Programmer\Hewlett-Packard\File Sanitizer*[Brugernavn]*_DiskBleachLog.txt

På 64-bit systemer er logfilerne placeret i følgende mapper på harddisken:

- C:\Programmer(x86)\Hewlett-Packard\File Sanitizer*[Brugernavn]*_ShredderLog.txt
- C:\Programmer(x86)\Hewlett-Packard\File Sanitizer*[Brugernavn]*_DiskBleachLog.txt

7 HP Device Access Manager (kun udvalgte modeller)

HP Device Access Manager kontrollerer adgangen til data ved at deaktivere dataoverførselsenheder.

BEMÆRK: Nogle grænseflader/inputenheder, såsom mus, tastatur, TouchPad og fingeraftrykslæser kontrolleres ikke af Device Access Manager. Se Ikke-administrerede enhedsklasser på side 45 for at få flere oplysninger.

Windows®-operativsystemadministratorer bruger HP Device Access Manager til at kontrollere adgangen til enhederne på et system og beskytte mod uautoriseret adgang:

- Enhedsprofiler oprettes for hver bruger, for at definere de enheder som de skal eller ikke skal have adgang til.
- Just In Time-godkendelse (JITA) gør det muligt for forud definerede brugere at få godkendelse til at tilgå enheder, som de ellers ikke har adgang til.
- Administratorer og anerkendte brugere kan ekskluderes fra begrænsninger for adgang til enheder indstillet i Device Access Manager ved at tilføje dem til enhedens administratorgruppe. Denne gruppes medlemskab styres ved hjælp af Avancerede indstillinger.
- Enhedsadgang kan gives eller nægtes på basis af gruppemedlemskab eller for individuelle brugere.
- Til flere kategorier som f.eks. cd-rom-drev og dvd-drev, kan læseadgang og skriveadgang tillades eller nægtes samtidig eller separat.

HP Device Access Manager konfigureres automatisk med de følgende indstillinger, når HP Client Security opsætningsguide gennemføres:

- Flytbare medier med Just In Time-godkendelse (JITA) er aktiveret for administratorer og brugere.
- Enhedspolitikken tillader fuld adgang til andre enheder.

Åbning af HP Device Access Manager

1. Fra startskærmen klikkes eller trykkes på appen **HP Client Security** (Windows 8).

   - eller -

   Fra Windows-skrivebordet, dobbeltklik eller dobbelttryk på ikonet **HP Client Security** i meddelelsesområdet, som er placeret længst til højre på proceslinjen.

2. Under **Enhed**, klik eller tryk på **Device Permissions** (Enhedstilladelser).

   - Standardbrugere kan se deres nuværende enhedsadgang (se Brugervisning på side 43).
   - Administrator kan se og ændre den enhedsadgang der for øjeblikket er konfigureret for computeren ved at klikke eller trykke på **Change** (Skift), og derefter indtaste administratoradgangskoden (se Systemvisning på side 43).

Brugervisning

Når **Device Permission**s (Enhedstilladelser) er valgt, vises brugervisningen. Alt afhængig af politikken, kan standardbrugere og administratorer se deres egen adgang til forskellige enhedsklasser eller til individuelle enheder på denne computer.

- **Aktuel bruger**—Navnet på den bruger, som for øjeblikket er logget ind, vises.
- **Enhedsklasse**—Enhedstyperne vises.
- **Adgang**—Din nuværende konfiguration for adgang forskellige typer af enheder eller specifikke enheder vises.
- **Varighed**—Tidsbegrænsningen for din adgang til cd/dvd-rom drev eller flytbar disk vises.
- **Indstillinger**—Administratorer kan angive de drev, for hvilke adgangen skal kontrolleres af Device Access Manager.

Systemvisning

I systemvisning kan administratorer tillade eller nægte adgang til enheder på denne computer for brugergruppen eller administratorgruppen.

▲ Administratorer kan få adgang til systemvisningen ved at klikke eller trykke på **Change** (Skift), indtaste en administrator-adgangskode og derefter vælge en af følgende muligheder:

- **Device Access Manager**—For at slå HP Device Access Manager med Just In Time-godkendelse til eller fra, klik eller tryk på **Til** eller **Fra**.
- **Brugere og grupper på denne PC**—Viser de brugergrupper eller administratorgrupper som enten har eller ikke har adgang til de valgte enhedsklasser.
- **Enhedsklasse**—Viser de enhedsklasser og enheder som er installeret på systemet eller som tidligere har været installeret på systemet. Klik på ikonet **+** for at udvide listen. Alle enheder som er sluttet til computeren vises, og administrator- og brugergrupper udvides, så deres medlemskab vises. Klik på ikonet med den runde pil (opdater), for at opdatere listen over enheder.
  - Beskyttelse gælder som regel for en enhedsklasse. Hvis adgang er indstillet til **Tillad**, har den valgte bruger adgang til enhver enhed i enhedsklassen.
  - Beskyttelse kan også gælde for specifikke enheder.
  - Konfigurer Just In Time-godkendelse (JITA), for at gøre det muligt for udvalgte brugere at få adgang til dvd/cd-rom drev eller flytbare diskdrev via en godkendelsesproces. Se JITA konfiguration på side 44 for at få flere oplysninger.
  - Tillad eller afvis adgang til andre enhedsklasser (såsom USB-flash drev), serielle og parallelle porte, Bluetooth®-enheder, modem-enheder, PCMCIA/ExpressCard-enheder, 1394-enheder, fingeraftrykslæsere, og chipkortlæsere. Hvis adgang til fingeraftrykslæser og chipkortlæser nægtes, kan de bruges som godkendelsesoplysninger, men de kan ikke bruges på session-politik-niveau.

    BEMÆRK: Hvis Bluetooth-enheder benyttes til godkendelsesoplysninger, skal man ikke begrænse adgangen til Bluetooth-enheder i Device Access Manager-politikken.

  - Når du vælger en indstilling på gruppe- eller enhedsklasse-niveau, og du bliver bedt om at angive en indstilling for de underordnede objekter:

    Ja—Indstillingen overføres.

Nej—Indstillingen overføres ikke.

- Nogle enhedsklasser, såsom dvd- og cd-rom, kan kontrolleres yderligere, ved at tilladelse eller afvisning af adgang til læsning og skrivning angives separat.

BEMÆRK: Gruppen Administratorer kan ikke tilføjes til brugerlisten.

- **Adgang**—Klik eller tryk på pil ned, og vælg derefter en af følgende adgangstyper for at tillade eller nægte adgang:
  - **Tillad—Fuld adgang**
  - **Tillad—Kun læsning**
  - **Tillad—JITA kræves**—For flere oplysninger, se JITA konfiguration på side 44.

    Klik eller tryk på pil ned under **Varighed** for at vælge en tidsbegrænsning, hvis denne adgangstype er valgt.
  - **Afvis**
- **Varighed**—Klik eller tryk på pil ned for at vælge en tidsbegrænsning for adgang til cd/dvd-rom drev eller flytbare diskdrev (se JITA konfiguration på side 44).

JITA konfiguration

JITA Configuration gør det muligt for administratoren at se og modificere lister over brugere og grupper som har adgang til enheder som benytter Just In Time-godkendelse (JITA).

JITA-aktiverede brugere kan få adgang til visse drev, som har politikker oprettet i visningen **Device Class Configuration** (Enhedsklassekonfigurering), der er blevet begrænset.

JITA-perioden kan godkendes til et antal minutter eller ubegrænset. Ubegrænsede brugere har adgang til enheden fra det tidspunkt hvor de logger på og indtil de logger af systemet igen.

Hvis brugeren får tildelt en begrænset JITA-periode, bliver brugeren et minut før JITA-perioden udløber, spurgt om adgangen skal forlænges. Så snart brugeren logger af systemet eller en anden bruger logger på, udløber JITA-perioden. Næste gang brugeren logger ind og forsøger at få adgang til en JITA-aktiveret enhed, bliver vedkommende bedt om at indtaste sine legitimationsoplysninger.

JITA er tilgængelig for følgende enhedsklasser:

- Dvd/cd-rom drev
- Flytbare diskdrev

Oprettelse af en JITA-politik for en bruger eller en gruppe

Administratorer kan give brugere eller grupper adgang til enheder ved hjælp af Just In Time-godkendelse (JITA).

1. Start **Device Access Manager**, og klik eller tryk derefter på **Change** (Skift).
2. Vælg brugeren eller gruppen, og klik eller tryk derefter på pil ned under **Access** (Adgang) for enten **Removable Disk drives** (Flytbare diskdrev) eller **dvd/cd-rom drev**, og vælg derefter **Allow – JITA Required** (Tillad – JITA krævet).
3. Klik eller tryk derefter på pil ned under **Duration** (Varighed), for at vælge en tidsbegrænsning for JITA-adgang.

Brugeren skal logge ud og logge ind igen, før den nye indstilling for JITA træder i kraft.

Deaktivering af en JITA-politik for en bruger eller en gruppe

Administratorer kan deaktivere brugeres eller gruppers adgang til enheder ved hjælp af Just In Time-godkendelse.

1. Start **Device Access Manager**, og klik eller tryk derefter på **Change** (Skift).
2. Vælg brugeren eller gruppen, og klik eller tryk derefter på pil ned under **Access** (Adgang) for enten **Removable Disk drives** (Flytbare diskdrev) eller **dvd/cd-rom drev**, og vælg derefter **Deny** (Afvis).

Når brugeren logger ind og forsøger at få adgang til enheden, bliver adgangen nægtet.

Indstillinger

Visningen **Indstillinger** gør det muligt for administratorer at se og ændre de drev, for hvilke adgangen skal kontrolleres af Device Access Manager.

BEMÆRK: Device Access Manager skal være aktiveret når listen over drevbogstaver konfigureres (se Systemvisning på side 43).

Ikke-administrerede enhedsklasser

HP Device Access Manager administrerer ikke følgende enhedsklasser:

- Input/output-enheder
  - Cd-rom
  - Diskdrev
  - Floppy-disk controller (FDC)
  - Harddisk controller (HDC)
  - Brugerstyret inputenhed (HID) klasse
  - Infrarød brugerstyret inputenhed
  - Mus
  - Multi-port seriel
  - Tastatur
  - Plug og Play (PnP) printere
  - Printer
  - Printer-opgradering
- Strøm-
  - Avanceret strømstyring (APM) support
  - Batteri
- Diverse
  - Computer
  - Dekoder
  - Skærm

- Intel® samlet skærmdriver
- Legacard
- Medie-driver
- Medie-skifter
- Hukommelsesteknologi
- Skærm
- Multifunktion
- Netklient
- Net-service
- Net-trans
- Processor
- SCSI-adapter
- Sikkerhedsaccelerator
- Sikkerhedsenheder
- System
- Ukendt
- Lydstyrke
- Øjebliksbillede af diskenhed

8 HP Trust Circles

HP Trust Circles er et sikkerhedsprogram til filer og dokumenter, som kombinerer mappe-filkryptering med en praktisk funktionalitet til deling af dokumenter i inden for en tillidscirkel. Programmet krypterer filer, som er placeret i brugerdefinerede mapper, og beskytter dem inden for en tillidscirkel. Når de først er omfattet af beskyttelsen, kan filerne kun bruges og deles af tillidscirklens medlemmer. Hvis en beskyttet fil modtages af en person som ikke er medlem af tillidscirklen, forbliver filen krypteret, og denne person kan ikke få adgang til indholdet.

Sådan åbnes Trust Circles

1. På startskærmen klikkes eller trykkes på appen **HP Client Security**.

   - eller -

   Fra Windows-skrivebordet, dobbeltklikkes på ikonet **HP Client Security** i meddelelsesområdet, som er placeret længst til højre på proceslinjen.

2. Under **Data**, klik eller tryk på **Trust Circles**.

Sådan kommer du i gang

Du kan sende invitationer pr. e-mail og besvare dem på to måder:

- **Ved hjælp af Microsoft® Outlook**—Behandlingen af Trust Circles invitationer og besvarelser fra andre brugere af Trust Circles kan automatiseres, hvis man bruger Trust Circles sammen med Microsoft Outlook.
- **Ved hjælp af Gmail, Yahoo, Outlook.com eller andre e-mail-tjenester (SMTP)**—Når du indtaster dit navn, din e-mailadresse og din adgangskode, bruger Trust Circles din e-mail-tjeneste til at sende e-mail-invitationer til de medlemmer der udvælges til at blive medlemmer af din tillidscirkel.

For at indstille din basis-profil:

1. Indtast dit navn og din e-mailadresse, og klik eller tryk derefter på **Næste**.

   Navnet kan ses af alle medlemmer, som inviteres til at slutte sig til din tillidscirkel. E-mailadressen bruges til at sende, modtage eller svare på invitationer.

2. Indtast adgangskoden til e-mail-kontoen, og klik eller tryk derefter på **Næste**.

   En test-e-mail sendes for at sikre at e-mail-indstillingerne er korrekte.

   BEMÆRK: Computeren skal være sluttet til et netværk.

3. Indtast et navn til tillidscirklen i feltet **Trust Circle Name** (Navn på tillidscirklen), og klik eller tryk derefter på **Næste**.

4. Tilføj medlemmer og mapper, og klik eller tryk derefter på **Næste**. Tillidscirklen oprettes med de mapper der blev valgt, og sender e-mail-invitationer ud til de medlemmer, som er blevet udvalgt. Hvis en invitation af en eller anden årsag ikke kan sendes, vises der en meddelelse. Medlemmer kan til enhver tid inviteres igen, ved at man i visningen Trust Circle klikker på **Your Trust**

Circles (Dine tillidscirkler), og derefter dobbeltklikker eller dobbelttrykker på tillidscirklen. Se Trust Circles på side 48 for at få flere oplysninger.

Trust Circles

Du kan oprette en tillidscirkel i forbindelse med den første opsætning, efter du har indtastet din e-mailadresse, eller i visningen Trust Circle:

▲ Fra visningen Trust Circle, klik eller tryk på **Create Trust Circle** (Opret tillidscirkel), og indtast derefter et navn til tillidscirklen.

- For at føje medlemmer til tillidscirklen, klik eller tryk på ikonet **M+** ved siden af **Members** (Medlemmer), og følg derefter anvisningerne på skærmen.
- For at føje mapper til tillidscirklen, klik eller tryk på ikonet **+** ved siden af **Folders** (Mapper), og følg derefter anvisningerne på skærmen.

Sådan føjes mapper til en tillidscirkel

Sådan føjes mapper til en ny tillidscirkel:

- I forbindelse med oprettelse af en tillidscirkel, kan du tilføje mapper ved at klikke eller trykke på ikonet **+** ved siden af **Mapper**, og derefter følge anvisningerne på skærmen.

  - eller -

- I Windows Stifinder kan du højreklikke eller trykke på og holde nede på en mappe som endnu ikke er en del af en tillidscirkel, vælge **Trust Circle** (Tillidscirkel), og derefter vælge **Create Trust Circle from Folder** (Opret tillidscirkel fra mappe).

TIP: Du kan vælge en eller flere mapper.

Sådan føjes mapper til en eksisterende tillidscirkel:

- Fra visningen Trust Circle, klik **Your Trust Circles** (Dine tillidscirkler), dobbeltklik eller dobbelttryk på den eksisterende tillidscirkel for at vise de nuværende mapper, klik eller tryk på ikonet **M+** ved siden af **Mapper**, og følg derefter anvisningerne på skærmen.

  - eller -

- I Windows Stifinder kan du højreklikke eller trykke på og holde nede på en mappe som endnu ikke er en del af en tillidscirkel, vælge **Trust Circle** (Tillidscirkel), og derefter vælge **Add to existing Trust Circle from Folder** (Føj til eksisterende tillidscirkel fra mappe).

TIP: Du kan vælge en eller flere mapper.

Når en mappe er blevet føjet til en tillidscirkel, krypterer Trust Circles automatisk mappen og dens indhold. Når alle filer er blevet krypteret, vises en meddelelse. Desuden vises et grønt symbol på alle ikoner for filer eller mapper der er krypteret inden for mapperne, hvilket indikerer at de er fuldt beskyttede.

Sådan føjes medlemmer til en tillidscirkel

Der er tre trin der skal udføres for at føje medlemmer til en tillidscirkel:

1. **Invitation**—Først inviterer ejeren af tillidscirklen medlemmet/medlemmerne. Invitations-e-mailen kan sendes til flere brugere eller til distributionslister eller -grupper.
2. **Accept**—Den inviterede part modtager invitationen og vælger om den skal accepteres eller afslås. Hvis den inviterede part accepterer invitationen, sendes et svar til invitationens afsender via e-mail. Hvis invitationen er blevet sendt til en gruppe, modtager hvert enkelt medlem en invitation, og kan vælge at acceptere eller afslå invitationen.
3. **Tilmed**—Den inviterende part, har en sidste mulighed for at beslutte om det nye medlem skal føjes til tillidscirklen. Hvis den inviterende part beslutter at tilmelde det nye medlem, får det nye medlem en e-mail, som bekræfter tilmeldingen. Den inviterende part og den inviterede part kan vælge at bekræfte invitationsprocessens sikkerhed. En bekræftelselseskode vises for den inviterede part. Denne kode skal læses op for den inviterende part over telefonen. Når koden er blevet bekræftet, kan den inviterende part sende den afsluttende tilmeldings-e-mail.

Sådan føjes medlemmer til en ny tillidscirkel:

▲ I forbindelse med oprettelse af en tillidscirkel, kan du tilføje medlemmer ved at klikke eller trykke på ikonet **M+** ved siden af **Members** (Medlemmer), og derefter følge anvisningerne på skærmen.

- Hvis du benytter Outlook, kan du vælge kontakter fra Outlook-adressebogen og derefter klikke på **OK**
- Hvis du benytter en anden e-mail-tjeneste, kan du enten tilføje nye e-mailadresser manuelt til Trust Circle, eller du kan indhente dem fra den e-mailadresse som er registreret på Trust Circle.

Sådan føjes medlemmer til en eksisterende tillidscirkel:

▲ Fra visningen Trust Circle, klik **Your Trust Circles** (Dine tillidscirkler), dobbeltklik eller dobbelttryk på den eksisterende tillidscirkel for at vise de nuværende mapper, klik eller tryk på ikonet **+** ved siden af **Members** (Medlemmer), og følg derefter anvisningerne på skærmen.

- Hvis du benytter Outlook, kan du vælge kontakter fra Outlook-adressebogen og derefter klikke på **OK**.
- Hvis du benytter en anden e-mail-tjeneste, kan du enten tilføje nye e-mailadresser manuelt til Trust Circle, eller du kan indhente dem fra den e-mailadresse som er registreret på Trust Circle.

Sådan føjes filer til en tillidscirkel

Du kan føje filer til en eksisterende tillidscirkel på en af følgende måder:

- Kopier eller flyt filen til en eksisterende tillidscirkel-folder.

  - eller -

- I Windows Stifinder, højreklik eller tryk på og hold en fil som endnu ikke er krypteret, vælg **Trust Circle**, og vælg derefter **Krypter**. Du vil blive bedt om at vælge den tillidscirkel som filen skal føjes til.

TIP: Du kan vælge en eller flere filer.

Krypterede mapper

Ethvert medlem af en tillidscirkel kan se og redigere de filer som hører til den pågældende tillidscirkel.

BEMÆRK: Trust Circle Manager/Reader (Tillidscirkel-administrator/Læser) synkroniserer ikke filer mellem medlemmer.

Filer skal deles med eksisterende metoder, som for eksempel e-mail, ftp eller cloud storage. Filer som kopieres til, flyttes til eller oprettes i en tillidscirkel beskyttes omgående.

Fjernelse af mapper fra en tillidscirkel

Fjernelse af en mappe fra en tillidscirkel dekrypterer mappen og hele dens indhold, og fjerner dermed beskyttelsen.

- Fra visningen Trust Circle, klik eller tryk på **Your Trust Circles** (Dine tillidscirkler), dobbeltklik eller dobbelttryk på den eksisterende tillidscirkel for at vise de nuværende mapper, klik eller tryk derefter på ikonet **trash can** (affaldsspand) ved siden af den pågældende mappe.

  - eller -

- I Windows Stifinder kan du højreklikke eller trykke på og holde nede på en mappe som for øjeblikket er en del af en tillidscirkel, vælge **Trust Circle** (Tillidscirkel), og derefter vælge **Remove from trust circle** (Fjern fra tillidscirkel).

TIP: Du kan vælge en eller flere mapper.

Fjernelse af en fil fra en tillidscirkel

For at fjerne en fil fra en tillidscirkel, skal du i Windows Stifinder højreklikke eller trykke og holde på en fil som er krypteret, vælge **Trust Circle**, og vælge **Dekrypter**.

Fjernelse af medlemmer fra en tillidscirkel

Et medlem som fuldt ud er blevet tilmeldt en tillidscirkel, kan ikke fjernes. Et alternativ kunne være at oprette en ny tillidscirkel indeholdende alle andre medlemmer, flytte alle filer og mapper til den nye tillidscirkel, og derefter slette den gamle tillidscirkel. Dette vil sikre at nye filer, som dette medlem modtager, ikke vil være tilgængelige, hvorimod alt det som tidligere er blevet delt, fortsat vil være tilgængeligt for medlemmet af den gamle tillidscirkel.

Hvis et medlem endnu ikke er fuldt ud optaget (enten er medlemmet blevet inviteret til at slutte sig til tillidscirklen, eller også har vedkommende ikke accepteret invitationen til tillidscirklen), kan du fjerne medlemmet fra tillidscirklen på en af følgende måder :

- Fra visningen Trust Circle, klik eller tryk på **Your Trust Circles** (Dine tillidscirkler), og dobbeltklik eller dobbelttryk derefter på tillidscirklen for at vise listen over de nuværende medlemmer. Klik eller tryk på ikonet **trash can** (affaldsspand) ved siden af navnet på det medlem som skal fjernes.
- Fra visningen Trust Circle, klik eller tryk på **Your Trust Circles** (Dine tillidscirkler), og dobbeltklik eller dobbelttryk derefter på medlemmet for at få vist de tillidscirkler, som vedkommende er medlem af. Klik eller tryk på ikonet **trash can** (affaldsspand) ved siden af en tillidscirkel for at fjerne medlemmet fra den tillidscirkel.

Sletning af en tillidscirkel

For at slette en tillidscirkel, skal man have ejerskab.

▲ Fra visningen Trust Circle, klik eller tryk på **Your Trust Circles** (Dine tillidscirkler), klik eller tryk på ikonet **trash can** (affaldsspand) ved siden af den tillidscirkel som skal slettes.

Dette fjerner tillidscirklen fra siden, og sender e-mails til alle medlemmer af tillidscirklen, som oplyser dem om at den pågældende tillidscirkel er blevet slettet. Alle filer eller foldere, som var en del af denne tillidscirkel dekrypteres.

Valg af indstillinger

Fra visningen Trust Circle, klik eller tryk på **Preferences** (Indstillinger). Der vises tre faneblade

- **E-mail-indstillinger**

Indstilling	Beskrivelse
Brugernavn	Det brugernavn, som for øjeblikket er i brug, vises. For at ændre det, skal man indtaste et nyt brugernavn i tekstfeltet. Ændringer gemmes automatisk.
E-mailadresse	Den e-mailadresse, som for øjeblikket er i brug, vises. For at ændre den, klik eller tryk på **Change Email Settings** (Rediger e-mail-indstillinger), og følg derefter anvisningerne på skærmen.
Bekræftelse af nye medlemmer	Vælg en af følgende valgmuligheder: ◦ **Confirm Automatically** (Bekræft automatisk)—Efter at modtage accept fra den eller de inviterede part(er), bekræftes de som medlemmer af tillidscirklen uden nogen form for manuelt indgriben, og en bekræftelses-e-mail sendes til den eller de inviterede part(er). ◦ **Confirm Manually** (Bekræft manuelt)—Efter at modtage accept fra den eller de inviterede part(er), kræves der manuel indgriben for at føje de nye medlemmer til tillidscirklen, hvorefter en bekræftelses-e-mail sendes til den eller de inviterede part(er). ◦ **Require Verification** (Kræv bekræftelse)—Efter at modtage accept fra den eller de inviterede part(er), kræves der en bekræftelseskode for fuldt ud at tilmelde den eller de inviterede part(er). Ejeren af tillidscirklen skal kontakte den eller de inviterede part(er) og modtage bekræftelseskoden fra dem. Når den korrekte kode er blevet indtastet, sendes bekræftelses-e-mails.
Periodic Authentication (Periodisk godkendelse)	Periodisk godkendelse kræver at brugeren indtaster adgangskoden til Windows efter en specificeret timeout-periode (måles i minutter) og også når der udføres følsomme handlinger. Denne indstilling gør det muligt for brugere at slå godkendelse til eller fra.
Authentication Timeout (Timeout for godkendelse)	Vælg den specificerede timeout-periode (måles i minutter), som skal gå, før godkendelse kræves.
Don't show confirmation message (Vis ingen bekræftelsesmeddelelse)	Vælg dette afkrydsningsfelt for at deaktivere visning af bekræftelsesmeddelelser, eller ryd afkrydsningsfeltet for at vise bekræftelsesmeddelelser.
I'd like to help improve the HP Trust Circle through anonymous usage tracking (Jeg vil gerne hjælpe med at forbedre HP Trust Circle gennem anonym brugssporing)	Vælg dette afkrydsningsfelt for at deltage i programmet, eller ryd afkrydsningsfeltet hvis du ikke ønsker at deltage.

- **Sikkerhedskopier/gendan**

Indstilling	Beskrivelse
Sikkerhedskopiering	Kopierer data fra programmet Trust Circle Manager/Reader (Tillidscirkel-administrator/Læser) (indstillinger og tillidscirkler) til en sikkerhedskopifil. I tilfælde af nedbrud eller systemfejl, kan du bruge denne fil til at gendanne din nye installation af Trust Circles til den tilstand, som er gemt i filen. **BEMÆRK:** Kun data fra programmet Trust Circle gemmes (tillidscirkler, indstillinger og medlemmer). Filerne i de mapper som hører til tillidscirklen sikkerhedskopieres ikke. Disse filer skal sikkerhedskopieres i en separat proces. For at sikkerhedskopiere indstillinger og brugerdata fra Trust Circles: **1.** Klik eller tryk på **Sikkerhedskopier**. **2.** Vælg et filnavn og en mappe til sikkerhedskopifilen, og klik eller tryk derefter på **Gem**. **3.** Indtast en adgangskode, bekræft den, og klik eller tryk derefter på **OK**. Denne adgangskode vil være påkrævet ved gendannelse af denne fil.
Gendanne	Gendanner indstillinger og tillidscirkler fra en sikkerhedskopifil, som regel efter et systemnedbrud eller ved overførsel til en anden computer. For at gendanne Trust Circle Manager's indstillinger og brugerdata: **1.** Klik eller tryk på **Restore** (Gendan). **2.** Naviger til sikkerhedskopifilens mappe og filnavn, og klik eller tryk derefter på **Åbn**. **3.** Indtast den adgangskode som blev angivet da sikkerhedskopien blev oprettet.

- **Om**—Trust Circle Manager/Reader-softwarens version vises. Der vises links, som gør det muligt at opgradere Trust Circle Manager til Pro-versionen eller at vise HP's fortrolighedserklæring.

9 Tyveri-gendannelse (kun udvalgte modeller)

Computrace (købes separat) giver dig mulighed for via fjernadgang at overvåge, styre og spore computeren.

Når Computrace aktiveres, er programmet konfigureret fra det absolutte software kundeservicecenter. Fra kundeservicecenteret kan administratoren konfigurere Computrace til at overvåge og administrere computeren. Hvis systemet bliver væk eller bliver stjålet, kan kundeservicecenteret hjælpe lokale myndigheder med at finde og gendanne computeren. Hvis konfigureret kan Computrace fortsætte med at fungere, selv hvis harddisken slettes eller udskiftes.

For at aktivere Computrace:

1. Opret forbindelse til internettet.
2. Åbn HP Client Security. Se Sådan åbnes HP Client Security på side 9 for at få flere oplysninger.
3. Klik på **Tyveri-gendannelse**.
4. For at starte Computrace aktiveringsguiden skal du klikke på **Kom godt i gang**.
5. Indtast dit kontaktoplysninger og dine kreditkortoplysninger eller indtaste en på forhånd købt produktnøgle.

Aktiveringsguiden behandler sikkert transaktionen og opsætter din brugerkonto på Absolut Software kundeservicecenters websted. Når det er gjort, modtager du en bekræftelses-e-mail med dine kundeservicecenter kontooplysninger.

Hvis du tidligere har kørt Computrace aktiveringsguiden, og din kundeservicecenter brugerkonto allerede findes, kan du købe ekstra licenser med at kontakte din HP-kunderepræsentant.

For at logge på kundeservicecenter:

1. Gå til https://cc.absolute.com/.
2. I felterne **login-ID** og **adgangskode** skal du indtaste legitimationsoplysningerne, du fik i bekræftelses-e-mail og derefter klikke på **Login**.

Ved hjælp af kundeservicecenteret, kan du:

- Overvåge dine computere.
- Beskytte dine data.
- Rapportere tyveri af enhver computer beskyttet af Computrace.

▲ Klik på **Flere oplysninger** for at få yderligere oplysninger om Computrace.

10 Lokaliserede adgangskode-undtagelser

På niveauerne opstartsgodkendelse og HP Drive Encryption er understøttelsen af lokaliserede adgangskoder begrænset. Se Windows IME'er, som ikke understøttes på niveauerne opstartsgodkendelse og HP Drive Encryption på side 54 for at få flere oplysninger.

Hvad man skal gøre, når en adgangskode afvises

Adgangskoder kan blive afvist af følgende årsager:

- Brugeren benytter en IME, som ikke understøttes. Dette er et udbredt problem ved sprog der benytter dobbelt-bytes (koreansk, japansk, kinesisk). For at løse problemet:
  1. Tilføj et understøttet tastaturlayout (tilføj tastaturet Engelsk (USA) under Kinesisk inputsprog) ved hjælp af **Kontrolpanel**.
  2. Indstil det understøttede tastatur som standard-tastatur.
  3. Start HP Client Security og indtast adgangskoden til Windows.
- Brugeren benytter et tegn, som ikke understøttes. For at løse problemet:
  1. Rediger adgangskoden til Windows, så den kun indeholder understøttede tegn. For flere oplysninger om tegn, som ikke understøttes, se Håndtering af specialtaster på side 55.
  2. Start HP Client Security og indtast adgangskoden til Windows.

Windows IME'er, som ikke understøttes på niveauerne opstartsgodkendelse og HP Drive Encryption

I Windows, kan brugeren vælge en IME (redigeringsprogram til input-metode) til at indtaste komplicerede tegn og symboler, såsom japanske eller kinesiske tegn, med et vestligt standardtastatur.

IME'er understøttes ikke på niveauerne opstartsgodkendelse og HP Drive Encryption. En adgangskode til Windows kan ikke indtastes med en IME på login-skærmene til opstartsgodkendelse eller HP Drive Encryption, og hvis man forsøger at gøre det, kan det føre til en situation hvor man ikke kan få adgang til systemet. I nogle tilfælde viser Microsoft® Windows ikke IME, når brugeren indtaster adgangskoden.

Løsningen består i at skifte til et af de følgende understøttede tastaturlayouts, som svarer til tastaturlayout 00000411:

- Microsoft IME til japansk
- Det japanske tastaturlayout
- Office 2007 IME til japansk—Hvis Microsoft eller en tredjepart bruger begrebet IME eller Input Method Editor (redigeringsprogram til input-metode), er det ikke sikkert at input-metoden rent faktisk er en IME. Dette kan skabe forvirring, men softwaren læser den hexadecimale kode som

ligger bag. Derfor kan HP Client Security understøtte konfigurationen, hvis IME'en er knyttet til et understøttet tastaturlayout.

ADVARSEL! Når HP Client Security er installeret, vil adgangskoder som indtastes med en Windows IME, blive afvist.

Ændring af adgangskoder ved hjælp af et tastaturlayout som også understøttes

Hvis adgangskoden oprindeligt indtastes med ét tastaturlayout, som for eksempel Engelsk (USA) (409), og brugeren derefter ændrer adgangskoden ved hjælp af et andet tastaturlayout som også understøttes, som for eksempel Latin-amerikansk (080A), vil den ændrede adgangskode fungere i HP Drive Encryption, men ikke i BIOS, hvis brugeren benytter tegn, som eksisterer i det første, men ikke i det sidste tastaturlayout (for eksempel ē).

BEMÆRK: Administratorer kan løse dette problem ved at benytte HP Client Security-siden Brugere (åbnes via ikonet **Gear** på startsiden) til at fjerne brugeren fra HP Client Security, vælge det ønskede tastaturlayout i operativsystemet og derefter køre opsætningsguiden HP Client Security Setup igen for den samme bruger. Det ønskede tastaturlayout gemmes i BIOS'en, og adgangskoder der kan indtastes med dette tastaturlayout, vil være korrekt indstillet i BIOS'en.

Et andet potentielt problem er brugen af forskellige tastaturlayouts, som kan frembringe de samme tegn. For eksempel kan både det internationale amerikanske tastaturlayout (20409) og det latin-amerikanske tastaturlayout (080A) frembringe tegnet é, selv om det muligvis kræver forskellige tastekombinationer. Hvis en adgangskode oprindeligt indtastes med det latin-amerikanske tastaturlayout, vil de latin-amerikanske tastaturlayout være indstillet i BIOS'en, selv om adgangskoden siden hen ændres ved hjælp af det internationale amerikanske tastaturlayout.

Håndtering af specialtaster

- Kinesisk, slovakisk, canadisk fransk og tjekkisk

  Når en bruger vælger et af de forudgående tastaturlayouts og derefter indtaster en adgangskode (f.eks. abcdef), skal den samme adgangskode indtastes, mens der trykkes på skift-tasten for små bogstaver og skift-tasten og caps lock-tasten for store bogstaver i opstartsgodkendelse og HP Drevkryptering. Numeriske adgangskoder skal indtastes med det numeriske tastatur.

- Koreansk

  Når en bruger vælger et tastaturlayout, der understøtter koreansk, og derefter indtaster en adgangskode, skal den samme adgangskode indtastes, mens der trykkes på højre alt-tast for små bogstaver og højre alt-tast og caps lock-tasten for store bogstaver i opstartsgodkendelse og HP Drevkryptering.

- Tegnene i nedenstående liste understøttes ikke:

Sprog	Windows	BIOS	Drive Encryption
Arabisk	Tasterne ﻯ ,ﻱ, og ﻯ frembringer to tegn.	Tasterne ﻯ ,ﻱ, og ﻯ frembringer et tegn.	Tasterne ﻯ ,ﻱ, og ﻯ frembringer et tegn.
Canadisk fransk	Ç, è, à og é med caps lock er Ç, È, À og É i Windows.	ç, è, à og é med caps lock er ç, è, à og é i opstartsgodkendelsen.	ç, è, à og é med caps lock er ç, è, à og é i HP Drive Encryption.

Sprog	Windows	BIOS	Drive Encryption
Spansk	40a understøttes ikke. Det fungerer alligevel, fordi softwaren konverterer det til c0a. På grund af små forskelle mellem disse tastaturlayouts, anbefales det alligevel at spansktalende brugere ændrer deres Windows-tastaturlayout til 1040a (spansk variation) eller 080a (latin-amerikansk).	Ikke relevant	Ikke relevant
Internationalt amerikansk	◦ Tasterne ¡, ¤, ‘, ’, ¥, og × på øverste række afvises. ◦ Tasterne å, ®, og Þ på anden række afvises. ◦ Tasterne á, ð, and ø på tredje række afvises. ◦ Tasten æ på nederste række afvises.	Ikke relevant	Ikke relevant
Tjekkisk	◦ Tasten ğ afvises. ◦ Tasten į afvises. ◦ Tasten ų afvises. ◦ Tasterne ė, ı, og ż afvises. ◦ Tasterne ģ, ķ, ļ, ņ, og ţ afvises.	Ikke relevant	Ikke relevant
Slovakisk	Tasten ż afvises.	◦ Tasterne š, ś, og ş afvises når de indtastes via tastaturet, men accepteres når de indtastes via softwaretastaturet. ◦ Den inaktive tast ţ frembringer to tegn.	Ikke relevant
Ungarsk	Tasten ż afvises.	Tasten ţ frembringer to tegn.	Ikke relevant
Slovensk	Tasten żŻ afvises i Windows, og alt-tasten frembringer en inaktiv tast i BIOS.	ú, Ú, ů, Ů, ş, Ş, ś, Ś, š, og Š afvises i BIOS.	Ikke relevant
Japansk	Hvis den er tilgængelig, er Microsoft Office 2007 IME et bedre valg. Selv om det kaldes en IME, er det i virkeligheden tastaturlayout 411, som understøttes.	Ikke relevant	Ikke relevant

Leksikon

administrator
Se *Windows-administrator*.

aktiv
En data-komponent som består af personlige oplysninger eller filer, historiske eller web-relaterede data og lignende, som er placeret på harddisken.

aktivering
Denne opgave skal gennemføres før nogen af funktionerne i Drive Encryption bliver tilgængelige. Administratorer kan aktivere Drive Encryption med HP Client Security opsætningsguiden eller med HP Client Security. Aktiveringsprocessen består af aktivering af softwaren, kryptering af drevet og oprettelse af den første sikkerhedskopi af krypteringsnøglen til en flytbar lagerenhed.

automatisk makulering
Makulering, som du planlægger i File Sanitizer.

Bluetooth
En teknologi, som benytter radio-transmissioner til på kort afstand at skabe kontakt til Bluetooth-aktiverede computere, printere, mus, mobiltelefoner og andre enheder til trådløs kommunikation.

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

chipkort
En hardwareenhed, som kan bruges til godkendelse sammen med en PIN-kode.

dekryptering
En procedure der anvendes kryptografi til at konvertere krypterede data til almindelig tekst.

domæne
En gruppe af computere, der er en del af et netværk og har en fælles mappedatabase. Domæner er entydigt navngivne, og hvert har en række fælles regler og procedurer.

Drive Encryption
beskytter dine data ved at kryptere dine harddiske, hvilket gør oplysningerne ulæsbare for dem uden korrekt tilladelse.

Drive Encryption før start-godkendelse.
En login-skærm som vises før Windows startes. Brugere skal indtaste deres Windows-brugernavn og -adgangskode eller PIN-kode til chipkort, eller stryge en registreret finger. Hvis one-step logon er valgt, vil indtastning af de korrekte oplysninger ved Drive Encryption login-skærmen give direkte adgang til Windows, uden man behøver at logge ind igen ved Windows login-skærmen.

Drive Encryption-logonskærm (Logonskærm for Drevkryptering)
Se Drive Encryption før start-godkendelse.

DriveLock
En sikkerhedsfunktion som linker harddisken til at en bruger og kræver, at brugeren indtaster korrekt DriveLock-adgangskode, når computeren starter.

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

enhedsklasse
Alle enheder af en bestemt type, som for eksempel drev.

Fingeraftryk
Et digitalt ekstrakt af et billede af dit fingeraftryk. Det faktiske billede af dit fingeraftryk gemmes aldrig af HP Client Security.

gendanne
En proces, der kopier programoplysninger fra en tidligere gemt sikkerhedskopifil i dette program.

genstart
Processen med genstart af computeren.

godkendelse
Den proces der ved hjælp af legitimationsoplysninger, deriblandt din adgangskode til Windows, dit fingeraftryk, et chipkort, et kontaktløst kort eller et nærhedskort, bekræfter at du virkelig er den person du hævder at være.

godkendelse ved start
En sikkerhedsfunktion, som kræver en form for godkendelse, f.eks. chipkort, sikkerhedschip eller adgangskode, når computeren tændes.

gruppe
En gruppe af brugere som tillades eller nægtes adgang til samme enhedsklasse eller til et specifikt drev.

hardware-kryptering
Brugen af selvkrypterende drev, som overholder Trusted Computing Group's OPAL-specifikationer for administration af selvkrypterende drev for fuldstændig og øjeblikkelig kryptering. Hardwarekryptering sker øjeblikkeligt og kan tage nogle få minutter, mens softwarekryptering kan tage flere timer.

HP SpareKey gendannelse
Muligheden for at få adgang til computeren ved at besvare sikkerhedsspørgsmål korrekt.

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

Id-kort
En Windows-skrivebords-gadget der har til formål visuelt at identificere dit skrivebord med dit brugernavn og valgte billede.

Just In Time-godkendelse
Se software-hjælpen til HP Device Access Manager.

kontaktløst kort
Et plastic-kort med en indbygget computer-chip, som kan benyttes til godkendelse.

Kryptering
En procedure, som f.eks. brug af en algoritme, der anvendes i kryptering til at konvertere almindelig tekst til krypteret tekst for at forhindre, at uautoriserede modtagere kan læse disse data. Der findes mange typer datakryptering, og de udgør grundlaget for netværkssikkerhed. Almindelige typer omfatter datakrypteringsstandard og kryptering med offentlig nøgle.

legitimationsoplysninger
En specifik information eller en hardwareenhed, som benyttes til at godkende en individuel bruger.

login
Et objekt i HP Client Security, som består af et brugernavn og en adgangskode (og muligvis andre valgte informationer), som kan benyttes til at logge ind på websider og andre programmer.

makulere
Udførelse af en algoritme, som overskriver de data som indeholdes i et aktiv med tilfældige data.

manuel makulering
Omgående makulering af et aktiv eller udvalgte aktiver, hvilket sker uden om en planlagt makulering.

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

nærhedskort
Et plastic-kort med en indbygget computer-chip, som i sammenhæng med andre oplysninger kan benyttes til godkendelse, for at skabe yderligere sikkerhed.

nødgendannelsesarkiv
Et beskyttet lagerområde der muliggør genkryptering af standardbrugernøgler fra en platform ejer-nøgle til en anden.

overskrivning af ledig plads
Overskrivning af slettede aktiver og ledig plads med tilfældige data. Denne proces reducerer eksistensen af det slettede aktiv, så det oprindelige aktiv bliver mere vanskeligt at gendanne.

PIN
Et personligt identifikationsnummer på en registreret bruger, som kan benyttes til godkendelse.

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

politik for enhedsadgangskontrol
Listen over enheder som brugeren tillades eller nægtes adgang til.

sikkerhedskopiere
Brugen af sikkerhedskopieringsfunktionen til at gemme en kopi af vigtige informationer fra et program til en placering uden for programmet. Den kan så benyttes til at gendanne informationerne på et senere tidspunkt, enten på den samme eller på en anden computer.

sikkerhedslogonmetode
Den metode, der anvendes til logon på computeren.

Single Sign On (Enkelt sign-on)
En funktion, der gemmer godkendelsesoplysninger og gør det muligt for dig at bruge HP Client Security til at få adgang til internettet og Windows-programmer, som kræver godkendelse af adgangskoder.

software-kryptering
Brugen af software til at kryptere harddisken sektor for sektor. Denne proces er langsommere end hardwarekryptering

Startside
En central placering, hvor du kan få adgang til og administrere funktioner og indstillinger i HP Client Security.

Tilsluttet enhed
En hardwareenhed, som er forbundet til en port på computeren.

TPM (Trusted Platform Module) integreret sikkerhedschip
En TPM godkender en computer i stedet for en bruger ved at opbevare oplysninger, som er specifikke for værtssystemet, f.eks. krypteringsnøgler, digitale certifikater og adgangskoder. En TPM minimerer risikoen for, at oplysninger på computeren vil blive kompromitteret efter en fysisk tyveri eller et angreb fra en ekstern hacker.

Trust Circle
Beskytter data ved at binde dem til en defineret gruppe af bruger, som der er tillid til. Dette forebygger at data falder i de forkerte hænder, enten ved et uheld eller med vilje. Data sikres med CryptoMill's Zero Overhead Key Management-teknologi og er kryptografisk bundet til en tillidscirkel. Dette forhindrer dekryptering af dokumenter eller andre følsomme oplysninger uden for tillidscirklen.

Trust Circle Manager/Reader (Tillidscirkel-administrator/Læser).
Trust Circle Reader (Tillidscirkel-læseren) kan kun acceptere invitationer, som er blevet sendt af brugere af Trust Circle Manager. Men Trust Circle Manager gør det muligt at oprette tillidscirkler. Man kan blandt andet invitere andre til en tillidscirkel via e-mail og acceptere invitationer til tillidscirkler fra andre. Når en tillidscirkel er oprettet, kan de filer, som beskyttes af denne cirkel, deles mellem medlemmerne på en sikker måde.

Trust Circle-mappe
Enhver mappe, som beskyttes af en tillidscirkel.

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

Windows-brugerkonto
En bruger som er autoriseret til at logge ind på et netværk eller på en individuel computer.

Windows login-sikkerhed
Beskytter dine Windows-konti ved at kræve brugen af specifikke legitimationsoplysninger for at få adgang.

Indeks