HP Client Security

Komme i gang

Første utgave: August 2013

Dokumentets delenummer: 735339-091

Innhold

1 Bruke HP Client Security Manager

HP Client Security lar deg beskytte dataen din, enheten din og identiteten din, og dermed øke sikkerheten på datamaskinen din.

Programvarens tilgjengelige oppgavemoduler til datamaskinen kan, variere avhengig av modell.

HP Clients programvaremoduler kan være forhåndsinstallert, forhåndslastet eller tilgjengelige for nedlasting fra HPs nettsted. Se http://www.hp.com for å få mer informasjon.

MERK: Instruksjonene i denne håndboken er skrevet med utgangspunkt i at du allerede har installert den aktuelle HP Client Security-modulene.

Funksjoner i HP Client Security

Tabellen nedenfor inneholder detaljert informasjon om viktige funksjoner i HP Client Security-modulene.

Modul	Hovedfunksjoner
HP Client Security Manager	Administratorer kan utføre følgende funksjoner: • Beskytte datamaskinen før Windows® starter opp • Beskytt Windows-kontoen med sterk godkjenning • Administrere brukernavn og passord for nettsteder og programmer • Endre passordet til Windows-operativsystemet enkelt • Bruke fingeravtrykk for ekstra sikkerhet og komfort • Sette opp et smartkort, kontaktfritt kort eller adgangskort for godkjenning • Bruke Bluetooth-telefonen som identifikasjonsmetode • Angi en PIN for å utvide din valg for godkjenning • Konfigurere pålogging og policyer for økter • Sikkerhetskopiere og gjenopprette programdata • Legge til flere programmer, som HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager og HP Computrace Generelle brukere kan utføre følgende funksjoner: • Vise på innstillingene for Krypteringsstatus og Device Access Manager. • Aktivere Computrace. • Konfigurere innstillinger og sikkerhetskopierings- og gjenopprettingsalternativer.

Modul	Hovedfunksjoner
Password Manager	Generelle brukere kan utføre følgende funksjoner: • Organisere og konfigurere brukernavn og passord. • Opprette mer solid passord for bedre sikkerhet på konto for e-post og Web kontoer. Passord Manager fyller automatisk ut informasjonen og sender den videre. • Effektiviser påloggingsprosessen med funksjonen Slingle Sign On, som automatisk husker og bruker påloggingsopplysningene dine. • Merke en konto som kompromittert, slik at du blir varslet for andre konti med lignende påloggingsinformasjon. • Importere påloggingdata fra en støttet nettleser.
HP Drive Encryption (kun på enkelte modeller)	• Gir komplett harddiskkryptering for hele disken. • Tvinger godkjenning før oppstart for å dekryptere og gi tilgang til data. • Gir muligheten til å aktivere selv-krypterende drivere (bare på enkelte modeller).
HP Device Access Manager	• Lar IT-sjefer kontrollere tilgang til enheter basert på brukerprofiler. • Forhindrer uautoriserte brukere i å fjerne data med eksterne lagringsmedier og i å introdusere virus i sytemet fra eksterne medier. • Gjør det mulig for administratorer å deaktivere tilgang til kommunikasjonsutstyr for bestemte enkeltpersoner og brukergrupper.
HP Trust Circles	• Sørger for fil- og dokumentsikkerhet. • Krypterer filer plassert i brukerdefinerte mapper og beskytter dem i en klarert sirkel. • Tillater kun bruk og deling av filer av medlemmer i den klarerte sirkelen.
Tyverigjenoppretting (Computrace, selges separat)	• Krever kjøp av eget sporingsabonnementer for å aktivere. • Sørger for sikker utstyrssporing. • Overvåker brukeraktivitet, i tillegg til endringer i maskinvare og programvare. • Forblir aktiv selv om harddisken er formatert eller skiftet ut.

Produktbeskrivelse og eksempler på bruk av HP Client

De fleste produkter fra HP Client Security har både brukergokjenning (vanligvis et passord) og administrativ sikkerhetskopi som gir tilgang hvis passordet er tapt, ikke tilgjengelig eller glemt, og hver gang bedriftens sikkerhet krever tilgang.

MERK: Noen av HP Client Security-produktene er utviklet for å begrense tilgang til data. Data skal være kryptert når det er så viktig at brukeren heller ville mistet informasjonen eller la den kompromitteres. Det anbefales at alle data sikkerhetskopieres på et sikkert sted.

Password Manager

Passord Manager lagrer brukernavn og passord, og kan brukes til følgende:

- Lagre påloggingsnavn og passord for tilgang til Internett og e-post.
- Automatisk logge brukeren på et nettsted eller en e-post.
- Administrere og organisere godkjenninger.
- Velge Internett- eller nettverksaktiva og gi direkte tilgang til koblingen.
- Vise navn og passord når det er nødvendig.
- Merke en konto som kompromittert, slik at du blir varslet for andre konti med lignende påloggingsinformasjon.
- Importere påloggingdata fra en støttet nettleser.

Eksempel 1: En innkjøpsrepresentant for en stor produsent foretar de fleste transaksjoner over Internett. Hun besøker også ofte populære nettsteder som krever pålogging. Hun er svært oppmerksom på sikkerhet, så hun unngår å bruke det samme passordet på hver konto. Innkjøpsrepresentanten har bestemt seg for å bruke Password Manager til å matche nettkoblinger med ulike brukernavn og passord. Når hun går til et nettsted for å logge på, presenterer Password Manager påloggingsinformasjonen automatisk. Hvis hun vil vise brukernavn og passord, kan Password Manager konfigurerres slik at disse vises.

Passord Manager kan også brukes til å administrere og organisere godkjenningerene. Dette verktøyet gir brukeren mulighet til å velge et nettverks- eller internettaktiva og gi direkte tilgang til koblingen. Brukeren kan også vise brukernavn og passord når det er nødvendig.

Eksempel 2: En hardtarbeidende ansatt er forfremmet og skal nå administrere hele regnskapsavdelingen,. Teamet må logge på et stort antall nettkonti tilhørende klienter, og hver av disse bruker ulik påloggingsinformasjon. Denne påloggingsinformasjonen må deles med andre brukere, så konfidensialitet er et problem. Den ansatte bestemmer seg for å organisere alle nettkoblinger, brukernavn, og passord i Passord Manager. Når prosessen er ferdig, gir den ansatte passord Manager til de ansatte, slik at de kan jobbe med nettkontiene uten noensinne å kjenne påloggingsinformasjonen de bruker.

HP Drive Encryption (kun på enkelte modeller)

HP Drive Encryption brukes til å begrense tilgang til data på hele datamaskinens harddisk eller en sekundær stasjon. Drive Encryption kan også administrere selvkrypterende stasjoner.

Eksempel 1: En lege vil sørge for at han er den eneste som har tilgang til data på datamaskinens harddisk. Legen aktiverer Drive Encryption, som krever gokjenning for Windows-pålogging før oppstart. Når den er konfigurert, gis det ikke tilgang til harddisken uten pasord før operativsystemet starter. Doktoren kunne så videre bedre stasjonens sikekrhet ved å vele å kryptere informasjonen med alternativet for selvkryptering.

Eksempel 2: En sykehusadministrator vil sørge for at kun leger og autorisert personell får tilgang til data på den lokale datamaskinen uten å dele personlige passord. IT-avdelingen legger til administratoren, leger og alt autorisert personell som brukere av Drive Encryption. Nå kan bare autorisert personell starte datamaskinen eller domenet med sine personlige brukernavn og passord.

HP Device Access Manager (bare på enkelte modeller)

HP Device Access Manager kan brukes av en administrator til å begrense og administrere tilgangen til maskinvare. Device Access Manager kan brukes til å blokkere uautorisert tilgang til USB-flash-stasjoner der data kan kopieres. Den kan også begrense tilgangen til CD-/DVD-stasjoner, styring av

USB-enheter, nettverkstilkoblinger, og så videre. Et eksempel vil være en situasjon der eksterne leverandører trenger tilgang til bedriftens datamaskiner, men bør ikke ha tilgang til å kopiere data til en USB-stasjon.

Eksempel 1: En sjefen i et legerekvisitaselskap jobber ofte med personlige legejournaler i forbinelse med selskapets informasjon. De ansatte trenger tilgang til denne informasjonen, men det er svært viktig at informasjonen ikke fjernes fra datamaskinen med USB-stasjon eller andre eksterne lagringsmedier. Nettverket er sikkert, men datamaskinene har CD-brennere og USB-porter som gjør det mulig å kopiere og stjele data. Sjefen bruker Device Access Manager til å deaktivere USB-porter og CD-brennere, slik at de ikke kan brukes. Selv om USB-portene er blokkert, fungerer fortsatt mus og tastatur.

Eksempel 2: Et forsikringsselskap vil unngå at de ansatte installerer eller laster inn personlig programvare hjemmefra. Noen ansatte trenger tilgang til USB-porten på alle datamaskiner. IT-administratoren bruker Device Access Manager for å gi tilgang for enkelte ansatte, samtidig som ekstern tilgang blokkeres for andre.

Computrace (kjøpes separat)

Computrace (kjøpes separat) er en tjeneste som kan lokalisere en stjålet datamaskin så lenge brukeren har tilgang til Internett. Computrace kan også fjernadministrere og lokalisere datamaskiner, samt overvåke databruk og applikasjoner.

Eksempel 1: En rektor har bedt IT-avdelingen om å holde oversikt med alle datamaskinene på skolen. Etter at datamaskininventaret ble sjekket, har IT-administratoren registrert alle datamaskinene med Computrace, slik at de kan spores hvis de skulle bli stjålet. Nylig fant skolen ut at flere datamaskiner manglet, så IT-administratoren meldte fra til myndighetene og funksjonærer fra Computrance. Datamaskinene ble lokalisert, og myndighetene returnerte dem til skolen.

Eksempel 2: Et eiendomsselskap har behov for å administrere og oppdatere datamaskiner over hele verden. De bruker Computrace til å overvåke og oppdatere datamaskiner uten å måtte sende IT-spesialister til hver enkelt maskin.

Oppnåelse av viktige sikkerhetsmål

HP Client Security-moduler fungerer sammen og skaper løsninger for en rekkel ulike sikkerhetsproblemer, inkludert følgende viktige sikkerhetsmål:

- Beskyttelse mot målrettet tyveri
- Begrensning av tilgang til sensitive data
- Forhindring av uautorisert tilgang fra interne og eksterne steder
- Oppretting av strengere krav til passordbeskyttelse

Beskyttelse mot målrettet tyveri

Et eksempel på et målrettet tyveri er tyveri av en datamaskin som inneholder konfidensiell informasjon og kundeinformasjon i sikkerhetskontrollen på flyplassen. Følgende funksjoner bidrar til å beskytte mot målrettet tyveri:

- Autoriseringsfunksjonen før oppstart, hvis den er aktivert, hjelper med å forhindre tilgang til operativsystemet.
  - HP Client Security—Se HP Client Security på side 12.
  - HP Drive Encryption—Se HP Drive Encryption (kun på enkelte modeller) på side 29.
- Kryptering bidrar til å hindre tilgang på data, selv om harddisken er tatt ut og installert på et usikret system.
- Computrace kan spore datamaskinens lokasjon etter et tyveri.
  - Computrace—Se Tyverigjenoppretting (kun på enkelte modeller) på side 53.

Begrensning av tilgang til sensitive data

La oss si at en ekstern revisor jobber på anlegget og har fått tilgang til datamaskinene for å gjennomgå sensitive økonomiske opplysninger. Du vil hindre at revioren skal kunne skrive ut filer eller lagre dem på en skrivbar enhet, for eksempel en CD. Følgende funksjon bidrar til å begrense tilgang til data:

- HP Device Access Manager lar IT-sjefer begrense tilgangen til kommunikasjonsenhetene, slik at sensitive opplysninger ikke kan kopieres fra harddisken. Se Systemvisning på side 43.

Forhindring av uautorisert tilgang fra interne og eksterne steder

Uoautorisert tilgang til en usikret datamaskin på arbeidsplasen utgjør en stor risiko for bedrifters nettverksressurser, for eksempel informasjon fra finanstjentster, en toppleder eller forsknings- og utviklingsteamet, og til privat informasjon som for eksempel pasientarkiver og personlig økonomiske arkiver. Følgende funksjoner bidrar til å forhindre uautorisert tilgang:

- Autoriseringsfunksjonen før oppstart, hvis den er aktivert, hjelper med å forhindre tilgang til operativsystemet. (se HP Drive Encryption (kun på enkelte modeller) på side 29).
- HP Client Security bidrar til at uautoriserte brukere ikke får passord eller tilgang til passordbeskyttede programmer. Se HP Client Security på side 12.
- HP Device Access Manager lar IT-sjefer for å begrense tilgangen til skrivbare enheter slik at sensitiv informasjon ikke kan kopieres fra harddisken. Se HP Device Access Manager (bare på enkelte modeller) på side 42.

Oppretting av strengere krav til passordbeskyttelse

Hvis en firmapolitikk iverksettes og krever bruk av en solid passordpolitikk for titalls nettbaerte applikasjoner og databaser, gir Password Manager et bekyttet lager for passord og enkel pålogging. Se Password Manager på side 18.

Ekstra sikkerhetselementer

Tildele sikkerhetsroller

Når det gjelder å administrere sikkerhet for datamaskiner (spesielt for store organisasjoner), er det viktig praksis å dele ansvaret og rettighetene på flere typer administratorer og brukere.

MERK: I en liten organisasjon eller til individuell bruk kan disse rollene innehas av samme person.

For HP Client Security kan dette sikkerhetsansvaret og privilegiene deles inn i følgende roller:

- Sikkerhetsansvarlig—Defines sikkerhetsnivået for selskapet eller nettveriket, og avgjør hvilke sikkerhetsfunksjoner som skal aktiveres, for eksempel Drive Encryption.

  MERK: Flere av funksjonene i HP Client Security kan spesialtilpasses av den sikkerhetsansvarlige i samarbeid med HP. Se http://www.hp.com for å få mer informasjon.

- IT-administrator—Påfører og administrerer sikkerhetsfunksjonene som er definert av den sikkerhetsansvarlige. Kan også aktivere og deaktivere visse funksjoner. Hvis for eksempel den sikkerhetsansvarlige har bestemt seg for å bruke smartkort, kan IT-administratoren aktivere både passord og smartkortmodus.
- Bruker—Bruker sikkerhetsfunksjonene. Hvis for eksempel den sikkerhesansvarlige og IT-administratoren har aktivert smartkort i systemet, kan brukeren angi PIN-kode for smartkortet og bruke kortet til godkjenning.

FORSIKTIG: Administratorer oppfordres til å følge "beste fremgangsmåter" når de skal begrense sluttbrukerens privilegier og begrense brukertilgang.

Uautoriserte brukere bør ikke ha gis administratorrettigheter.

Administrasjon av HP Client Security-passord

De fleste funksjonene i HP Client Security er passordbeskyttet. Tabellen nedenfor viser vanlige passorde, programvaremodul der passordet er angitt og passordfunksjonen.

Passordene som opprettes og brukes kun av IT-administratorer angis også i denne tabellen. Alle andre passord kan angis av vanlige brukerne og administratorer.

HP Client Security-passord	Angi i følgende modul	Funksjon
Windows-påloggingspassord	Windows Kontrollpanel eller HP Client Security	Kan brukes til manuell pålogging og til godkjenning for å få tilgang til ulike HP Client Security-funksjoner.
HP Client Security Backup og gjenopprettingspassord	HP Client Security, av individuell bruker	Beskytter tilgang til HP Client Security Backup og gjenopprettingsfil.
Smartkortkode	Credential Manager (legitimasjonsbehandling)	Kan brukes som flerfaktorautentisering. Kan brukes som Windows-autorisering. Autentiserer brukere av Drive Encryption, hvis smartkort er valgt.

Opprett et sikkert passord

Når du oppretter passord, må du følge alle spesifikasjoner som er angitt av programmet. Generelt, bør du likevel ta hensyn til følgende retningslinjer for å hjelpe deg med å lage solide passord og redusere faren for at passordet blir kompromittert:

- Bruk passord med mer enn 6 tegn, og helst mer enn 8.
- Veksle mellom store og små bokstaver i hele passordet.
- Om mulig, veksle mellom alfanumeriske tegn og inkluder spesialtegn og skilletegn.
- Bruk spesialtegn eller tall for istedenfor vanlige bokstaver i viktige ord. Du kan for eksempel bruke tallet 1 til å repreentere bokstavene I og L.
- Kombinere ord fra to eller flere språk.
- Del et ord eller en frase med tall og spesialtegn i midten, for eksempel "Mary2-2Cat45."
- Ikke bruk passord som finnes i ordboken.
- Ikke bruk navnet ditt som passord, eller annen personlig informasjon, for eksempel fødselsdatoen din, navn på kjæledyr eller din mors pikenavn, selv om du staver det baklengs.
- Bytt passord med jevne mellomrom. Du kan endre bare et par tegn som trinn.
- Hvis du skriver ned passordet, må du ikke lagre det på steder der det vanligvis er synlig i nærheten av datamaskinen.
- Ikke lagre passordet i en fil, for eksempel en e-post, på datamaskinen.
- Ikke del kontoer eller del passordet ditt med noen.

Sikkerhetskopiering av påloggingsopplysninger og innstillinger

Du kan bruke sikkerhetskopierings og gjenoppretningsverktøyet i HP Client Security som en sentral for sikkerhetskopiering og gjenoppretting av sikkerhetspåloggingsinformasjon fra noen av de installerte HP Client Security-modulene.

2 Komme i gang

For å konfigurere HP Client Security for bruk med din påloggingsinformasjon, starter du HP Client Security på én av følgende måter. Når veiviseren er fullført av en bruker, kan den ikke startes igjen av den samme brukeren.

1. Fra startskjermen eller skjermen med apper klikker eller trykker du på **HP Client Security**-appen (Windows 8).

   – eller –

   Fra Windows-skrivebordet klikker eller trykker du på **HP Client Security**-miniprogrammet (Windows 7).

   – eller –

   Fra Windows-skrivebordet dobbeltklikker eller dobbelttrykker du på **HP Client Security**-ikonet i systemstatusfeltet, som du finner helt til høyre på oppgavelinjen.

   – eller –

   Fra Windows-skrivebordet klikker eller trykker du på **HP Client Security**-ikonet i systemstatusfeltet, og velger **Open HP Client Security** (Åpne HP Client Security).

2. Installasjonsveiviseren for HP Client Security åpnes og viser deg velkomstsiden.

3. Les det som står på velkomstskjermen, verifiser identiteten din ved å skrive inn Windows-passordet ditt og klikk eller trykk på **Next** (Neste).

   Hvis du ennå ikke har opprettet et Windows-passord, blir du bedt om å gjøre det. Et Windows-passord er nødvendig for å beskytte Windows-kontoen fra uautoriserte personer, og for å kunne bruke HP Client Security-funksjonene.

4. På HP SpareKey-siden velger du tre sikkerhetsspørsmål. Skriv inn et svar for hvert spørsmål, og klikk deretter **Next** (Neste). Egendefinerte spørsmål er også tillatt. Se HP SpareKey—Gjenoppretting av passord på side 14 for å få mer informasjon.

5. På Fingeravtrykk-siden registrerer du minst det nødvendige antallet fingeravtrykk, og klikker eller trykker deretter på **Next** (Neste). Se Fingeravtrykk på side 12 for å få mer informasjon.

6. På Drive Encryption-siden aktiverer du kryptering, tar sikkerhetskopi av krypteringsnøkkelen og klikker eller trykker på **Next** (Neste). For mer informasjon, se programvarehjelpen i HP Drive Encryption.

   MERK: Dette gjelder for et scenario der brukeren er administrator, og installasjonsveiviseren til HP Client Security ikke har blitt konfigurert av en administrator tidligere.

7. På den siste siden til veiviseren, klikker eller trykker du på **Finish** (Fullfør).

   Denne siden viser deg status til funksjoner og legitimasjon.

8. Installasjonsveiviseren til HP Client Security Setup sørger for å aktivere Just In Time Authentication- og File Sanitizer-funksjonen. For mer informasjon, se programvarehjelpen til HP Device Access Manager og HP File Sanitizer.

   MERK: Dette gjelder for et scenario der brukeren er administrator, og installasjonsveiviseren til HP Client Security ikke har blitt konfigurert av en administrator tidligere.

Åpne HP Client Security

Du kan åpne HP Client Security-program på følgende måter:

MERK: Installasjonsveiviseren for HP Client Security må være gjennomført før HP Client Security-programmet kan åpnes.

- Fra startskjermen eller skjermen med apper klikker eller trykker du på **HP Client Security**-appen.

  – eller –

  Fra Windows-skrivebordet klikker eller trykker du på **HP Client Security**-miniprogrammet (Windows 7).

  – eller –

  Fra Windows-skrivebordet dobbeltklikker eller dobbelttrykker du på **HP Client Security**-ikonet i systemstatusfeltet, som du finner helt til høyre på oppgavelinjen.

  – eller –

  Fra Windows-skrivebordet klikker eller trykker du på **HP Client Security**-ikonet i systemstatusfeltet, og velger **Open HP Client Security** (Åpne HP Client Security).

3 Enkel installeringsveiledning for små bedrifter

Dette kapittelet er laget for å demonstrere de grunnleggende trinnene for å aktivere de vanligste og nyttigste alternativene i HP Client Security for små bedrifter. Mange av verktøyene for i denne programvaren lar deg finjustere innstillinger og stiller inn tilgangskontroll. Fokus i denne enkle installeringsveiledning er å få hver modul igang med minst mulig tid brukt på installasjon. Hvis du vil ha mer informasjon, velger du modulen du er interessert i, og klikker deretter på **?** eller Hjelp-knappen øverst til høyre. Denne knappen viser automatisk all informasjon for å hjelpe med det aktiverte vinduet.

Komme i gang

1. Fra Windows-skrivebordet åpner du HP Client Security ved å dobbeltklikke på **HP Client Security**-ikonet i systemstatusfeltet, helt til høyre på oppgavelinjen.
2. Skriv inn Windows-passordet eller opprette et Windows-passordet.
3. Fullfør installasjonen av HP Client Security.

Vil du at HP Client Security kun skal kreve godkjenning én gang i løpet av Windows-påloggingen, se Security-funksjoner på side 26.

Password Manager

Alle har et antall passord - spesielt hvis de med jevne mellomrom bruker webområder eller applikasjoner som krever pålogging. Den vanlige brukeren bruker enten det samme passordet for hver applikajon eller nettsted, eller blir kreativ og glemmer fort hvilket passord som hører til hvilket program.

Passord Manager kan automatisk huske passord eller gi deg muligheten til å skille mellom hvilke nettsteder som skal huskes og hvilke som skal utelates. Når du har logget deg på datamaskinen, gir Password Manager deg passord og påloggingsinformasjon til deltakende programmer og nettsteder.

Når du åpner et program eller et nettsted som krever påloggingsinformasjon, gjenkjenner Password Manager nettstedet automatisk og spør deg om du vil at programvaren skal huske informasjonen din. Hvis du vil ekskludere bestemte områder, kan du avslå forespørselen.

For å lagring av webområder brukernavn og passord:

1. For eksempel, gå til et deltakende nettsted eller applikasjon, og klikk på Password Manager-ikonet øverst i venster hjørne på webområdet for å legge til nettgodkjenning.
2. Gi koblingen et navn (frivillig) og angi et brukernavn og passord i Passord Manager.
3. Når du er ferdig, klikker du på **OK**-knappen.
4. Passord Manager kan også lagre brukernavn og passord for nettverksdeling og tilordnede nettverkstasjoner.

Vise og administrere lagrede godkjenninger i Passord Manager

Passord Manager gir deg muligheten til å vise, behandle, sikkerhetskopiere og starte godkjenninger sentralt. Passord Manager støtter også oppstart av lagrede nettsteder fra Windows.

For å åpne passord Manager, bruker du tastekombinasjonen Ctrl+Windows-tasten+h for åpne Password Manager, og deretter klikker du på **Log in** for å starte og godkjenne den lagrede snarveien.

Passord Managers **redigerings**-alternativ lar deg vise og endre navn, påloggingnavn og til og med vise passord.

HP Client Security tillater sikkerhetskopiering og/eller kopiering av alle godkjenninger og innnstillinger til en annen datamaskin.

HP Device Access Manager

Device Access Manager kan brukes til å begrense bruken av ulike interne og eksterne lagringsenheter slik at dataene vil være sikre på harddisken, og ikke går ut døren i bedriften. Et eksempel er å gi en bruker tilgang til dine data, men blokkere dem fra kopiering til CD, personlig musikkspiller og USB-enheter.

1. Åpne **Device Access Manager** (se Åpne Device Access Manager på side 42).

   Tilgang for gjeldende bruker vises.

2. For å endre tilgang for brukere, grupper eller enheter, klikker du eller trykker på **Endre**. Se Systemvisning på side 43 for å få mer informasjon.

HP Drive Encryption

HP Drive Encryption brukes til å beskytte data ved å kryptere hele harddisken på nytt. Data på harddisken forblir beskyttet hvis PC-en er skulle bli stjålet og/eller hvis harddisken blir fjernet fra den opprinnelige datamaskinen og plasseres i en annen datamaskin.

En ekstra sikkerhetsfordel er at Drive Encryption krever at du godkjenner bruk av brukernavn og passord før operativsystemet starter. Denne prosessen kalles godkjenning før oppstart.

For å gjøre det enkelt for deg, synkroniseres flere programvaremoduler passord automatisk, inkludert brukerkontoer for Windows, godkjenningsdomener, HP Drive Encryption, Password Manager og HP Client Security.

For installasjon av HP Drive Encryption ved første installasjon av HP Client Security-installasjonsveiviseren, se Komme i gang på side 8.

4 HP Client Security

Hjem-siden til HP Client Security er det sentrale stedet for enkel tilgang til funksjonene, programmene og innstillingene i HP Client Security. Hjemmesiden er delt inn i tre seksjoner:

- **DATA**—Gir tilgang til programmer brukt for håndtering av datasikkerhet.
- **DEVICE** (ENHET)—Gir tilgang til programmer brukt for håndtering av enheters sikkerhet.
- **IDENTITY** (IDENTITET)—Lar deg registrere og administrere godkjenning av legitimasjon.

Flytt markøren over et program for å vise en beskrivelse av programmet.

HP Client Security kan gi koblinger til brukerinnstillinger og administrative innstillinger på bunnen av siden. HP Client Security gir tilgang til avanserte innstillinger og funksjoner ved å trykke eller klikk på **tannhjul** (innstillinger)-ikonet.

Identitetsfunksjoner, programmer og innstillinger

Identitetsfunksjoner, programmer og innstillinger tilgjengelig gjennom HP Client Security hjelper deg med å administrere ulike aspekter ved den digitale identiteten din. Klikk eller trykk på en av de følgende flisene på Hjem-siden til HP Client Security, og skriv inn Windwos-passordet ditt:

- **Fingerprints** (Fingeravtrykk)—Registrer og administrer legitimasjon med fingeravtrykk.
- **SpareKey**—Setter opp og administrerer din HP SpareKey-legitimasjon, som kan brukes for å logge på datamaskinen hvis andre måter for legitimasjon er mistet eller forlagt. Du kan også tilbakestille ditt glemte passord.
- **Windows Password** (Windows-passord)—Gir deg enkelt muligheten til å endre Windows-passordet ditt.
- **Bluetooth Devices** (Bluetooth-enheter)—Lar deg registrere og administrere dine Bluetooth-enheter.
- **Cards** (Kort)—Lar deg registrere og administrere dine smartkort, kontaktfrie kort og nærhetskort.
- **PIN**—Lar deg registrere og administrere PIN-kode for legitimasjon.
- **RSA SecurID**-lar deg registrere og administrere RSA SecurID-påloggingsinformasjon (hvis riktig oppsett er foretatt).
- **Password Manager** (Passordadministrator)—Lar deg administrere passordene dine for online kontoer og programmer.

Fingeravtrykk

Installasjonsveiviseren til HP Client Security guider deg gjennom prosessen med å sette opp, eller "registrere", fingeravtrykkene dine.

Du kan også registrere eller slette fingeravtrykkene dine på Fingeravtrykk-siden, som du får tilgang til ve på klikke eller trykke på **Fingerprints** (Fingeravtrykk)-ikonet på Hjem-siden til HP Client Security.

1. På Fingeravtrykk-siden sveiper du en finger til den er registrert.

   Antall fingre som kreves for å bli registrert er angitt på siden. Peke- eller langefingeren foretrekkes.

2. For å slette tidligere registrerte fingeravtrykk, klikk eller trykk på **Delete** (Slett).

3. For å registrere ekstra fingeravtrykk, klikk eller trykk på **Enroll an additional fingerprint** (Registrer et ekstra fingeravtrykk).

4. Klikk på eller trykk på **Save** (Lagre) før du forlater siden.

⚠ **FORSIKTIG:** Når du registrerer fingeravtrykk gjennom veiviseren, vil ikke fingeravtrykket lagres før du klikker på **Next** (Neste). Hvis du lar datamaskinen være inaktiv en stund, eller lukker programmet, vil endringer du har gjort **ikke** lagres.

- ▲ For å få tilgang til de administrative innstillingene for fingeravtrykk, hvor administratorer kan spesifisere registrering, nøyaktighet og andre innstillinger, klikk eller trykk på **Administrative Settings** (Administrative innstillinger) (krever administratorrettigheter).
- ▲ For å få tilgang til brukerinnstillingene for fingeravtrykk, hvor du kan spesifisere innstillinger som styrer gjenkjenning av fingeravtrykk og oppførsel, klikk eller trykk på **User Settings** (Brukerinnstillinger).

Administrative innstillinger for fingeravtrykk

Administratorer kan spesifisere registrering, nøyaktighet og andre innstillinger for en fingeravtrykkleser. Administratorrettigheter er nødvendig.

- ▲ For å få tilgang til administrative innstillinger for legitimasjon med fingeravtrykk, klikk eller trykk på **Administrative Settings** (Administrative innstillinger) på Fingeravtrykk-siden.

- **User enrollment** (Brukerregistrering)—Velg minimum og maksimum antall fingeravtrykk en bruker kan registrere.
- **Recognition** (Gjenkjenning)—Flytt glidebryteren for å justere sensitiviteten som brukes av fingeravtrykkleseren når du sveiper fingeren din.

  Hvis fingeravtrykket ditt ikke gjenkjennes hele tiden, må du kanskje velge en lavere innstilling for gjenkjenning. En høyere innstilling øker følsomheten for variasjoner i avlesingen av fingeravtrykk, og minsker derfor faren for at fingeravtrykket er falskt. **Medium-High** (Medium/Høy)-innstillingen gir en god avveining mellom sikkerhet og brukervennlighet.

Brukerinnstillinger for fingeravtrykk

På siden med brukerinnstillinger for fingeravtrykk kan du spesifisere innstillingene som styrer gjenkjenning av fingeravtrykk og oppførsel.

▲ For å få tilgang til brukerinnstillinger for legitimasjon med fingeravtrykk, klikk eller trykk på **User Settings** (Brukerinnstillinger) på Fingeravtrykk-siden.

- **Enable sound feedback** (Aktiver tilbakemelding med lyd)—Som standard gir HP Client Security deg tilbakemelding med lyd når et fingeravtrykk har blitt sveipet, og spiller av forskjellige lyder for spesifikke programhendelser. Du kan tildele nye lyder til disse hendelsene gjennom Lyder-kategorien under Lyder-innstillingene i Windows-kontrollpanelet. Hvis du vil deaktivere tilbakemelding med lyd, fjerner du merket i boksen.
- **Show scan quality feedback** (Vis tilbakemelding på skanningens kvalitet)—For å vise alle sveip, uavhengig av kvalitet, velg avmerkingsboksen. For å vise bare sveip med bra kvalitet, fjerner du merket i boksen.

HP SpareKey—Gjenoppretting av passord

HP SpareKey lar deg få tilgang til datamaskinen din (på støttede plattformer) ved å svare på tre sikkerhetsspørsmål.

HP Client Security ber deg om å sette opp din personlige HP SpareKey første gang du kjører installasjonsveiviseren for HP Client Security.

For å sette opp HP SpareKey:

1. På HP SpareKey-siden i veiviseren velger du tre sikkerhetsspørsmål, og oppgir deretter et svar for hvert av spørsmålene.

   Du kan velge et spørsmål fra en forhåndsdefinert liste, eller skrive dine egne spørsmål.

2. Klikk eller trykk på **Enroll** (Registrer).

For å slette din HP SpareKey:

▲ Klikk eller trykk på **Delete your SpareKey** (Slett din SpareKey).

Etter at din SpareKey er satt opp, kan du få tilgang til datamaskinen din ved å benytte din SpareKey fra en påloggingsskjerm som vises når du slår på datamaskinen eller på velkomstskjermen til Windows.

Du kan velge ulike spørsmål eller endre svarene dine på SpareKey-siden, som du får tilgang til fra Gjenoppretting av passord-flisen på Hjem-siden til HP Client Security.

For å få tilgang til HP SpareKey-innstillinger, hvor en administrator kan spesifisere innstillinger relatert til HP SpareKey-legitimasjon, klikk på **Settings** (Innstillinger) (krever administratorrettigheter).

HP SpareKey Settings

På siden HP SpareKey-innstillinger kan du spesifisere innstillinger som styrer oppførselen og bruken av HP SpareKey-legitimasjon.

▲ For å åpne siden med HP SpareKey-innstillinger, klikk eller trykk på **Settings** (Innstillinger) på HP SpareKey-siden (krever administratorrettigheter).

Administratorer kan velge følgende innstillinger:

- Spesifiser spørsmålene som presenteres for hver bruker under oppsettet av HP SpareKey.
- Legge til opptil tre egendefinerte sikkerhetsspørsmål som legges til i liste som presenteres for brukerne.
- Velg om du vil tillate at brukere skriver inn sine egne sikkerhetsspørsmål.
- Spesifisere hvilke godkjenningsmiljøer (Windows-godkjenning eller godkjenning ved oppstart) som tillater bruk av HP SpareKey for gjenoppretting av passord.

Windows-passord

HP Client Security gjør det enklere og raskere å endre Windows-passordet ditt, i forhold til å benytte Windows-kontrollpanelet.

For å endre Windows-passordet:

1. Fra Hjem-siden til HP Client Security klikker eller trykker du på **Windows Password** (Windows-passord).
2. Skriv inn det gjeldende passordet i **Current Windows password** (Gjeldende Windows-passord)-tekstboksen.
3. Skriv inn et nytt passord i **New Windows password** (Nytt Windows-passord)-tekstboksen, og skriv det deretter på nytt igjen i **Confirm new password** (Bekreft nytt passord)-tekstboksen.
4. Klikk eller trykk **Change** (Endre) for å umiddelbart endre passordet ditt til det nye du skrev inn.

Bluetooth-enheter

Hvis administratoren har aktivert Bluetooth som godkjenning av legitimasjon, kan du sette opp en Bluetooth-telefon i forbindelse med annen legitimasjon for ekstra sikkerhet.

MERK: Kun telefoner med Bluetooth støttes.

1. Sørg for at Bluetooth-funksjonen er aktivert på datamaskinen, og at Bluetooth-telefonen er satt i oppdagelsesmodus. For å koble til telefonen, må du kanskje skrive inn en automatisk generert kode på Bluetooth-enheten. Avhengig av Bluetooth-enhetens konfigurasjonsinnstillinger, kan en sammenligning av paringskoder mellom datamaskinen og telefonen være nødvendig.
2. For å registrere telefonen, velger du den og klikker eller trykker på **Enroll** (Registrer).

For å få tilgang til Innstillinger for Bluetooth-enheter på side 15-siden, hvor en administrator kan spesifisere innstillingene for Bluetooth-enheter, klikk **Settings** (Innstillinger) (krever administratorrettigheter).

Innstillinger for Bluetooth-enheter

Administratorer kan spesifisere følgende innstillinger som styrer oppførselen og bruken av Bluetooth-enhet til legitimasjon:

Stille godkjenning

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity** (Bruker automatisk din tilkoblede, registrerte Bluetooth-enhet under godkjenningen av identiteten din)—Velg avmerkingsboksen for å la brukere bruker Bluetooth-enhet som legitimasjon for godkjenning uten å kreve en handling fra brukeren, eller fjern haken i avmerkingsboksen for å deaktivere dette alternativet.

Bluetooth-nærhet

- **Låse datamaskinen når den registrerte Bluetooth-enheten er utenfor datamaskinens rekkevidde.**—Velg avmerkingsboksen for å låse datamaskinen når en Bluetooth-enheter som ble koblet til under påloggingen er utenfor rekkevidde, eller fjern haken i avmerkingsboksen for å deaktivere dette alternativet.

MERK: Bluetooth-modulen på datamaskinen din må støtte denne mulighet for at du skal kunne benytte deg av funksjonen.

Kort

HP Client Security kan støtte en rekke forskjellige typer ID-kort, som er små kort av plastikk som inneholder en databrikke. Dette inkluderer smartkort, kontaktfrie kort og nærhetskort. Hvis et av disse kortene, og den aktuelle kortleseren, er koblet til datamaskinen, og hvis administratoren har installert den tilknyttede driveren fra produsenten og aktivert kortet som en godkjenning av legitimasjon, kan du bruke kortet som en godkjenning av legitimasjon.

For smartkort tilbyr produsenten verktøy som lar deg installere et sikkerhetssertifikat og PIN-administrasjon, som HP Client Security bruker i sin sikkerhetsalgoritmen. Antall og type tegn som brukes som PIN kan variere. En administrator må initialisere smartkortet før det kan brukes.

Følgende smartkortformater støttes av HP Client Security:

- CSP
- PKCS11

Følgende typer kontaktfrie kort støttes av HP Client Security:

- Kontaktløse HID iCLASS-minnekort
- Kontaktløse MiFare Classic 1k, 4k og miniminnekort

Følgende typer nærhetskort støttes av HP Client Security:

- HID-nærhetskort

For å registrere et smartkort:

1. Sett kortet inn i en tilknyttet smartkortleser.
2. Når kortet gjenkjennes skriver du inn PIN-korden, og klikker eller trykker på **Enroll** (Registrer).

For å endre PIN-koden på et smartkort:

1. Sett kortet inn i en tilknyttet smartkortleser.
2. Når kortet gjenkjennes skriver du inn PIN-korden, og klikker eller trykker på **Authenticate** (Godkjenn).
3. Klikk eller trykk **Change PIN** (Endre PIN-kode), og skriv deretter inn den nye PIN-koden.

For å registrere et kontaktfritt kort eller nærhetskort:

1. Plasser kortet på eller veldig nær den aktuelle leseren.
2. Når kortet gjenkjennes, klikk eller trykk på **Enroll** (Registrer).

For å slette et registrert kort:

1. Presenter kortet til leseren.
2. For smartkort skriver du inn kortets tildelte PIN-korden, og klikker eller trykker på **Authenticate** (Godkjenn).
3. Klikk eller trykk på **Delete** (Slett).

Når kortet er registrert, vises detaljer om kortet under **Enrolled Cards** (Registrerte kort). Når et kort slettes, fjernes det fra listen.

For å få tilgang til innstillingene for nærhetskort, kontaktfrie kort og smartkort, hvor administratoren kan spesifisere innstillinger relatert til kortlegitimasjon, klikk eller trykk på **Settings** (Innstillinger) (krever administratorrettigheter).

Innstillinger for nærhetskort, kontaktfrie kort og smartkort

For å få tilgang til innstillingene for et kort, klikk eller trykk på kortet i listen, og klikk eller trykk deretter på pilen som vises.

For å endre PIN-koden på et smartkort:

1. Presenter kortet til leseren
2. Skriv inn kortets tildelte PIN-kode, og klikk eller trykk på **Continue** (Fortsett).
3. Skriv inn og bekreft den nye PIN-korden, og klikk eller trykk på **Continue** (Fortsett).

For å initialisere PIN-koden på et smartkort:

1. Presenter kortet til leseren
2. Skriv inn kortets tildelte PIN-kode, og klikk eller trykk på **Continue** (Fortsett).
3. Skriv inn og bekreft den nye PIN-korden, og klikk eller trykk på **Continue** (Fortsett).
4. Klikk eller trykk **Yes** (Ja) for å bekrefte initialiseringen.

For å fjerne dataen på kortet:

1. Presenter kortet til leseren
2. Skriv inn kortets tildelte PIN-kode (kun for smartkort), og klikk eller trykk på **Continue** (Fortsett).
3. Klikk eller trykk **Yes** (Ja) for å bekrefte slettingen.

PIN-kode

Hvis administratoren har aktivert PIN-kode som godkjenning av legitimasjon, kan du sette opp en PIN-kode i forbindelse med annen legitimasjon for ekstra sikkerhet.

Slik stiller du inn ny PIN-kode:

▲ Skriv inn PIN-koden, skriv den inn igjen for å bekrefte og klikk eller tapp **Apply** (Bruk).

For å slette en PIN-kode:

▲ Klikk eller trykk **Delete** (Slett), og klikk eller trykk **Yes** (Ja) for å bekrefte.

For å få tilgang til PIN-innstillingene, hvor administratoren kan spesifisere innstillinger relatert til PIN-legitimasjon, klikk eller trykk på **Settings** (Innstillinger) (krever administratorrettigheter).

PIN Settings

På siden PIN-innstillinger kan du spesifisere minimum og maksimal lengde på PIN-koden som brukes for legitimasjon.

RSA SecurID

Hvis administratoren har aktivert RSA som en godkjenning av legitimasjon, og følgende betingelser er oppfylte, kan du registrere eller slette en RSA SecurID-legitimasjon.

MERK: Riktig oppsett er nødvendig.

- Brukeren må være opprettet på en RSA-server.
- RSA SecurID-brikken tilordnet brukeren og datamaskinen må ha vært knyttet til RSA-serverens domene.
- SecurID-programvare er installert på datamaskinen.
- En kobling er tilgjengelig til den riktig konfigurerte RSA-serveren.

For å registrere en RSA SecurID-legitimasjon:

▲ Skriv inn brukernavnet og koden din for RSA SecurID (kode fra RSA SecurID-brikke eller PIN +kode fra brikke, avhengig av miljøet ditt), og klikk eller trykk **Apply** (Bruk).

Etter vellykket registrering vises meldingen: "Din RSA SecurID-legitimasjon har blitt registrert", og Slett-knappen aktiveres.

For å slette en RSA SecurID-legitimasjon:

▲ Klikk **Delete** (Slett), og velg deretter **Yes** (Ja) i boksen som spør deg "Er du sikker på at du vil slette din RSA SecurID-legitimasjon?".

Password Manager

Det er både enklere og tryggere å logge seg inn på nettsteder og programmer når du bruker Password Manager. Du kan opprette sterkere passord som du ikke trenger skrive ned eller huske, og logge deg på enkelt og raskt med en fingeravtrykkleser, et smartkort, et nærhetskort, et kontaktfritt kort, en Bluetooth-telefon, en PIN-kode, RSA-legitimasjon eller et Windows-passord.

MERK: På grunn av de stadige endringene av sidene på nettsteder hvor du logger deg på, kan ikke Password Manager større alle nettsteder.

Password Manager tilbyr følgende alternativer:

Password Manager-side

- Klikk eller trykk på en konto for å automatisk åpne et nettsted eller program og logge deg på.
- Bruk kategorier til å organisere kontoene dine.

Passordstyrke

- Se med et raskt blikk om noen av passordene dine utgjør en sikkerhetsrisiko.
- Når du legger til påloggingsinformasjon, sjekkes styrken til individuelle passord som brukes for nettsteder eller programmer.
- Passordets styrke illustreres av røde, gule eller grønne statusindikatorer.

Password Manager-ikonet vises øverst i høyre hjørne av påloggingsskjermen til nettstedet eller programmet. Når påloggingsinformasjon enda ikke har blitt opprettet for et nettsted eller et program, vil et pluss-tegn vises på ikonet.

▲ Klikk eller trykk på **Password Manager**-ikonet for å vise en hurtigmeny hvor du kan velge følgende alternativer:

- Legg til [etdomene.no] til Password Manager
- Åpne Password Manager
- Innstillinger for ikon
- Hjelp

For nettsteder eller programmer hvor påloggingsinformasjon ikke har blitt opprettet

Følgende alternativer vises på hurtigmenyen:

- **Add [somedomain.com] to the Password Manager** (Legg til [etdomene.no] til Password Manager)—Lar deg legge til en pålogging for den gjeldende påloggingsskjermen.
- **Open Password Manager** (Åpne Password Manager)—Åpner Password Manager.
- **Icon Settings** (Innstillinger for ikon)—Lar deg spesifisere når **Password Manager**-ikonet skal vises.
- **Help** (Hjelp)—Vises hjelpen til HP Client Security.

For nettsteder eller programmer hvor påloggingsinformasjon allerede har blitt opprettet

Følgende alternativer vises på hurtigmenyen:

- **Fill in logon data** (Fyll inn påloggingsinformasjon)—Viser en **Verify your identity** (Verifiser din ID)-side. Hvis du godkjennes vil din påloggingsinformasjon plasseres i påloggingsfeltene, og du logges inn på siden (hvis innlogging var spesifisert da påloggingen ble opprettet eller sist endret).
- **Edit Logon** (Endre pålogging)—Lar deg endre påloggingsinformasjonen for nettstedet.
- **Add Logon** (Legg til pålogging)—Lar deg legge en konto til Password Manager.
- **Open Password Manager** (Åpne Password Manager)—Åpner Password Manager.
- **Help** (Hjelp)—Vises hjelpen til HP Client Security.

MERK: Administratoren for denne datamaskinen kan ha konfigurert HP Client Security til å kreve mer enn én legitimasjon ved verifisering av identiteten din.

Legge til påloggінger

Du kan enkelt legge til en pålogging for et nettsted eller et program ved å skrive inn påloggingsinformasjon én gang. Fra da av vil Password Manager automatisk legge inn informasjonen for deg. Du kan bruke disse påloggingene etter å ha gått til nettstedet eller programmet.

For å legge til en pålogging:

1. Åpne påloggingsskjermen for et nettsted eller program.
2. Klikk eller trykk på **Password Manager**-ikonet, og klikk eller trykk deretter på en av følgende, avhengig av om påloggingsskjermen er for et nettsted eller et program:
   - For et nettsted, klikk eller trykk **Add [domain name] to Password Manager** (Legg [domenenavn] til Password Manager).
   - For et program, klikk eller trykk **Add this logon screen to Password Manager** (Legg denne påloggingsskjermen til Password Manager).
3. Skriv inn påloggingsdataene. Påloggingsfeltene på skjermen, og de tilsvarende feltene i dialogboksen, identifiseres med en tykk, oransje kant.
   a. For å fylle ut et påloggingsfelt med en av de på forhånd formaterte valgene, klikk eller trykk på pilene til høyre for feltet.
   b. For å vise passordet for denne pålogging, klikk eller trykk på **Show password** (Vis passord).
   c. For å fylle inn påloggingsfeltene, men ikke sende inn informasjonen, fjern **Automatically submit logon data** (Send automatisk inn påloggingsinformasjon).
   d. Klikk eller trykk på **OK** for å velge godkjenningsmetoden som du ønsker å bruke (fingeravtrykk, smartkort, nærhetskort, kontaktfrie kort, Bluetooth-telefon, PIN-kode eller passord), og logg deretter på med den valgte godkjenningsmetoden.

      Pluss-tegnet fjernes fra **Passord Manager**-ikonet for å varsle deg om at pålogging er opprettet.
   e. Hvis Password Manager ikke oppdater noen påloggingsfelter, klikk eller trykk på **More fields** (Flere felter).
      - Merk av for hvert felt som kreves ved pålogging, eller opphev merkingen av alle felter som ikke kreves ved pålogging.
      - Klikk eller trykk på **Close** (Lukk).

Hver gang du går til det nettstedet eller åpner det programmet, vil **Password Manager**-ikonet vises øverst i venstre hjørne på et nettsted eller påloggingsskjermen til et program, noe som indikerer at du kan bruke din registrerte informasjon til å logge deg på.

Endre påloggінger

For å endre en pålogging:

1. Åpne påloggingsskjermen for et nettsted eller program.
2. For å vise en dialogboks hvor du kan endre påloggingsinformasjonen din, klikk eller trykk på **Password Manager**-ikonet og klikk eller trykk deretter på **Edit Logon** (Endre pålogging).

   Påloggingsfeltene på skjermen, og de tilsvarende feltene i dialogboksen, identifiseres med en tykk, oransje kant.

   Du kan også endre kontoinformasjon på Password Manager-siden. Klikk eller trykk på påloggingen for å vise alternativene for å endre, og velg **Edit** (Endre).

3. Endre påloggingsinformasjonen din.

   - For å endre **Account name** (Kontonavn), skriver du et nytt navn i feltet.
   - For å legge til eller endre en **Category** (Kategori), skriver du inn eller endrer navnet i **Category** (Kategori)-feltet.
   - For å velge et **Username** (Brukernavn)-påloggingsfelt med en av de på forhånd formaterte valgene, klikk eller trykk på pil ned til høyre for feltet.

     Forhåndsformaterte valg er bare tilgjengelige når du endrer påloggingen fra Endre-kommandoen i hurtigmenyen til Passord Manager-ikonet.
   - For å velge et **Passowrd** (Passord)-påloggingsfelt med en av de på forhånd formaterte valgene, klikk eller trykk på pil ned til høyre for feltet.

     Forhåndsformaterte valg er bare tilgjengelige når du endrer påloggingen fra Endre-kommandoen i hurtigmenyen til Passord Manager-ikonet.
   - For å legge til andre felter fra skjermen til påloggingen din, klikker eller trykker du på **More fields** (Flere felter).
   - For å vise passordet for denne pålogging, klikk eller trykk på **Show password** (Vis passord)-ikonet.
   - For å fylle inn påloggingsfeltene, men ikke sende inn informasjonen, fjern **Automatically submit logon data** (Send automatisk inn påloggingsinformasjon).
   - For å markere at denne påloggingen har et utsatt passord, velg **This password is compromised** (Dette passordet er utsatt)-avmerkingsboksen.

     Etter at endringene er lagret, vil alle andre påloggingen som deler det samme passordet også merkes som utsatt. Du kan deretter gå til hver berørte konto og endre passordet hvis ønskelig.

4. Klikk eller trykk på **OK**.

Bruke Password Managers meny med hurtigkoblinger

Password Manager gir en rask og enkel måte å åpne nettsteder og programmer hvor du har opprettet påloggingen på. Dobbeltklikk eller dobbelttrykk på en pålogging til et program eller nettsted fra **Password Manager Quick Links** (Hurtigkoblinger for Password Manager), eller fra Password Manager-siden i HP Client Security, for å åpne påloggingsskjermen og fylle inn påloggingsinformasjonen din.

Når du oppretter en pålogging legges den automatisk til i Password Managers **Quick Links** (Hurtigkoblinger)-meny.

For å vise **Quick Links** (Hurtigkoblinger)-menyen:

▲ Trykk på **Password Manager**-hurtigtastkombinasjonen (Ctrl+Windows-tast+h er fabrikkinnstillingen). For å endre hurtigtastkombinasjon fra Hjem-siden til HP Client Security, klikker du **Password Manager** etterfulgt av **Settings** (Innstillinger).

Organisere påloggingene i kategorier

Opprett én eller flere kategorier for å holde orden på påloggingene din.

For å tilordne en pålogging til en kategori:

1. Fra Hjem-siden til HP Client Security klikker eller trykker du på **Password Manager**.
2. Klikk eller trykk på en oppført konto, og klikk eller trykk deretter på **Edit** (Endre).

3. I **Category** (Kategori)-feltet skriver du inn et navn på kategorien.
4. Klikk eller trykk på **Save** (Lagre).

For å fjerne en konto fra en kategori:

1. Fra Hjem-siden til HP Client Security klikker eller trykker du på **Password Manager**.
2. Klikk eller trykk på en oppført konto, og klikk eller trykk deretter på **Edit** (Endre).
3. I **Category** (Kategori)-feltet sletter du navnet på kategorien.
4. Klikk eller trykk på **Save** (Lagre).

For å gi en kategori et nytt navn:

1. Fra Hjem-siden til HP Client Security klikker eller trykker du på **Password Manager**.
2. Klikk eller trykk på en oppført konto, og klikk eller trykk deretter på **Edit** (Endre).
3. I **Category** (Kategori)-feltet ender du navnet på kategorien.
4. Klikk eller trykk på **Save** (Lagre).

Administrere dine påloggінger

Password Manager gjør det enkelt å administrere din påloggingsinformasjon for brukernavn, passord og flere påloggingskontoer, alt fra ett sted.

Påloggingene dine er listet opp på Password Manager-siden.

For å administrere påloggingene dine:

1. Fra Hjem-siden til HP Client Security klikker eller trykker du på **Password Manager**.
2. Klikk eller trykk på en eksisterende pålogging, og velg deretter ett av følgende alternativer, og følg instruksjonene på skjermen:
   - **Edit** (Endre)—Endre en pålogging. Se Endre påloggінger på side 20 for å få mer informasjon.
   - **Log in** (Logg inn)—Logg inn på den valgte kontoen.
   - **Delete** (Slett)—Slett påloggingen for den valgte kontoen.

For å legge til en ekstra pålogging for et nettsted eller program:

1. Åpne påloggingsskjermen for nettstedet eller programmet.
2. Klikk eller trykk på **Password Manager**-ikonet for å vise hurtigmenyen.
3. Klikk eller trykk på **Add Logon** (Legg til pålogging), og følg instruksjonene på skjermen.

Vurdering av passordstyrken

Det er viktig å bruke sterke passord på nettsteder og programmer for å beskytte identiteten din.

Password Manager gjør overvåking og forbedring av sikkerheten din til en enkel sak, med umiddelbar og automatisert analyse av styrken til hvert av passordene du bruker til å logge deg på dine nettsteder og programmer.

Når du skriver inn et passord under opprettelsen av Password Manager-påloggingen for en konto, vil en farget linje vises under passordet som angir passordstyrken. Fargene angir følgende verdier:

- **Rød**—Svakt
- **Gul**—Greit nok
- **Grønn**—Sterkt

Innstillinger for Password Manager-ikon

Password Manager prøver å identifisere påloggingsskjermer for nettsteder og programmer. Når det oppdager en påloggingsskjerm hvor du ikke har opprettet en pålogging, vil Password Manager be deg opprette en pålogging for skjermen ved å vise **Passord Manager**-ikonet med et pluss-tegn på seg.

1. Klikk eller trykk på ikonet, og klikk eller trykk deretter på **Icon Settings** (Innstillinger for ikon) for å tilpasse hvordan Password Manager håndterer mulig sider med pålogging.
   - **Prompt to add logons for logon screens** (Bli bedt om å legge til påloggінger for påloggingsskjermer)—Klikk eller trykk på dette alternativet for å få Password Manager til å be deg om å legge til en pålogging når en påloggingsskjerm vises og du ikke allerede har en pålogging for den.
   - **Exclude this screen** (Ekskluder denne skjermen)—Velg avmerkingsboksen så Password Manager ikke spør deg om å lage en pålogging for denne påloggingsskjermen igjen.
   - **Do not prompt to add logons for logon screens** (Ikke bli bedt om å legge til påloggінger for påloggingsskjermer)—Velg radioknappen.
2. For å legge til en pålogging for en skjerm som tidligere har blitt ekskludert:
   a. Logg på det tidligere ekskluderte nettstedet.
   b. For å få Password Manager til å huske passordet for denne siden, klikker eller trykker du på Remember (Husk) i dialogboksen som dukker opp, og passordet vil husker og en pålogging opprettes for den skjermen.
3. For å få tilgang til flere Password Manager-innstillinger, klikk eller trykk på Passord Manager-ikonet, klikk eller trykk på **Open Password Manager** (Åpne Password Manager) og klikk eller trykk på **Settings** (Innstillinger) på Password Manager-siden.

Import og eksport av påloggінger

På HP Password Managers Import og eksport-side kan du importere påloggінger lagret av nettleseren på datamaskinen. Du kan også importere data fra en HP Client Security-sikkerhetskopi og eksportere data til en HP Client Security-sikkerhetskopi.

▲ For å åpne Import og eksport-siden klikker eller trykker du på **Import and export** (Import og eksport) på Password Manager-siden.

For å importere passord fra en nettleser:

1. Klikk eller trykk på nettleseren du ønsker å importere passord fra (kun installerte nettlesere vises).
2. Fjern haken i avmerkingsboksen for alle kontoer du ikke vil importere passord fra.
3. Klikk på eller tapp **Importer**.

Importering av data fra, eller eksportering av data til, en HP Client Security-sikkerhetskopi kan gjøres gjennom de tilknyttede koblingene (under **Other Options** (Andre alternativer)) på Import og eksport-siden.

MERK: Denne funksjonen importerer og eksporterer bare Password Manager-data. For informasjon om sikkerhetskopiering og gjenoppretting av annen HP Client Security-data, se Sikkerhetskopiere og gjenopprette dataen din på side 28.

For å importere data fra en HP Client Security-sikkerhetskopifil:

1. Fra HP Password Manager sin Import og eksport-side, klikker eller trykker du på **Import data from an HP Client Security backup file** (Importer data fra en HP Client Security-sikkerhetskopifil).
2. Bekreft identiteten din.
3. Velg den tidligere opprettede sikkerhetskopifilen eller angi banen i feltet som vises, og klikk eller trykk deretter på **Browse** (Bla gjennom).
4. Skriv inn passordet som ble brukt til å beskytte filen, og klikk eller trykk på **Next** (Neste).
5. Klikk eller trykk på **Restore** (Gjenopprett).

For å eksportere data til en HP Client Security-sikkerhetskopifil:

1. Fra HP Password Manager sin Import og eksport-side, klikker eller trykker du på **Export data to an HP Client Security backup file** (Eksporter data til en HP Client Security-sikkerhetskopifil).
2. Verifiser identiteten din og klikk eller trykk på **Next** (Neste).
3. Skriv inn et navn for sikkerhetskopifilen. Som standard lagres filen i Dokumenter-mappen din. For å spesifisere en annen lokasjon, klikk eller trykk på **Browse** (Bla gjennom).
4. Skriv inn og bekreft et passord for å beskytte filen, og klikk eller trykk på **Save** (Lagre).

Innstillinger

Du kan spesifisere innstillinger for tilpassing av Password Manager:

- **Prompt to add logons for logon screens** (Bli bedt om å legge til påloginger for påloggingsskjermer)—**Password Manager**-ikonet med et pluss-tegn på seg vises når påloggingsskjermen til et nettsted eller program oppdages, noe som indikerer at du kan legge en pålogging for denne skjermen i **Logons** (Påloginger)-menyen.

  For å deaktivere denne funksjonen, fjerner du haken i avmerkingsboksen ved siden av **Prompt to add logons for logon screens** (Be om å legge til påloginger for påloggingsskjermer).

- **Åpne passord Manager med Ctrl+Win+h**- standard direktetasten som åpner **Passord Manager-koblinger**-menyen er Ctrl+Windows-tasten+h.

  For å endre hurtigtast, klikk eller trykk på dette alternativet, og trykk deretter inn en ny tastekombinasjon. Kombinasjoner kan omfatte én eller flere av følgende: Ctrl, alt, eller shift, og hvilken som helst alfanumerisk tast.

  Kombinasjoner forbeholdt Windows eller Windows-programmer kan ikke brukes.

- For å gå tilbake til standardinnstillingen, klikk eller trykk på **Restore defaults** (Gjenopprett standardinnstillinger).

Avanserte innstillinger

Administratorer kan få tilgang til følgende alternativer ved å velge **tannhjul**-ikonet på Hjem-siden til HP Client Security.

- **Administrator Policies** (Policyer for administrator)—Lar deg konfigurere policyer for pålogging og økter for administratorer.
- **Standard User Policies** (Policyer for vanlige brukere)—Lar deg konfigurere policyer for pålogging og økter for vanlige brukere.
- **Security Features** (Sikkerhetsfunksjoner)—Lar deg øke sikkerheten til datamaskinen din ved å beskytte Windows-konto med sterkgodkjenning og/eller ved å aktivere godkjenning før Windows starter.
- **Users**-lar deg administrere brukere og påloggingsinformasjon.
- **My Policies** (Mine policyer)—Lar deg se gjennom policyene for godkjenning og status for registrering.
- **Backup and Restore** (Sikkerhetskopi og gjenoppretting)—Lar deg ta sikkerhetskopi eller gjenopprette data for HP Client Security.
- **Om HP Client Security**—viser versjonsinformasjon om HP Client Security.

Policyer for administrator

Du kan konfigurere policyer for pålogging og økter for administratorer på denne datamaskinen. Policyer for pålogging angitt her styrer legitimasjonen som er påkrevd for at lokale administratorer skal kunne logge seg på Windows. Policyer for økter angitt her styrer legitimasjonen som er påkrevd for at lokale administratorer skal verifisere identiteten sin i en Windows-økt.

Som standard håndheves alle nye og endrede policyer umiddelbart etter at du har klikket eller trykket på **Apply** (Bruk).

For å legge til en ny policy:

1. Fra Hjem-siden til HP Client Security klikker eller trykker du på **tannhjul**-ikonet.
2. På siden Avanserte innstillinger klikker eller trykker du på **Administrator Policies** (Policyer for administratorer).
3. Klikk eller trykk på **Legg til ny policy**.
4. Klikk på pil ned for å velge primær og (valgfritt) sekundær legitimasjon for nye policyer, og klikk eller trykk på **Add** (Legg til).
5. Klikk på **Bruk**.

For å forsinke iverksetting av en ny eller endret policy:

1. Klikk eller trykk på **Enforce this policy immediately** (Håndhev denne policyen umiddelbart).
2. Velg **Enforce this policy on the specific date** (Håndhev denne policyen på en gitt dato).
3. Skriv inn eller bruke kalenderen som dukker opp til å velge en dato for når denne policyen skal håndheves.
4. Om ønskelig, kan du velge når brukerne skal minnes på denne nye policyen.
5. Klikk på **Bruk**.

Policyer for vanlige brukere

Du kan konfigurere policyer for pålogging og økter for vanlige brukere på denne datamaskinen. Policyer for pålogging angitt her styrer legitimasjonen som er påkrevd for at vanlige brukere skal kunne logge seg på Windows. Policyer for økter angitt her styrer legitimasjonen som er påkrevd for at vanlige brukere skal verifisere identiteten sin i en Windows-økt.

Som standard håndheves alle nye og endrede policyer umiddelbart etter at du har klikket eller trykket på **Apply** (Bruk).

For å legge til en ny policy:

1. Fra Hjem-siden til HP Client Security klikker eller trykker du på **tannhjul**-ikonet.
2. På siden Avanserte innstillinger klikker eller trykker du på **Standard User Policies** (Policyer for vanlig bruker).
3. Klikk eller trykk på **Legg til ny policy**.
4. Klikk på pil ned for å velge primær og (valgfritt) sekundær legitimasjon for nye policyer, og klikk eller trykk på **Add** (Legg til).
5. Klikk på **Bruk**.

For å forsinke iverksetting av en ny eller endret policy:

1. Klikk eller trykk på **Enforce this policy immediately** (Håndhev denne policyen umiddelbart).
2. Velg **Enforce this policy on the specific date** (Håndhev denne policyen på en gitt dato).
3. Skriv inn eller bruke kalenderen som dukker opp til å velge en dato for når denne policyen skal håndheves.
4. Om ønskelig, kan du velge når brukerne skal minnes på denne nye policyen.
5. Klikk på **Bruk**.

Security-funksjoner

Du kan aktivere HP Client Security-funksjoner som bidrar til å beskytte mot uautorisert tilgang til datamaskinen.

For å sette opp sikkerhetsfunksjoner:

1. Fra Hjem-siden til HP Client Security klikker eller trykker du på **tannhjul**-ikonet.
2. På siden Avanserte innstillinger klikker eller trykker du på **Security Policies** (Sikkerhetspolicyer).

3. Aktiver sikkerhetsfunksjoner ved å merke avmerkingsboksene, og klikk eller trykk deretter på **Apply** (Bruk). Jo flere funksjoner du velger, desto sikrere blir maskinen.

   Disse innstillingene gjelder for alle brukere.

   - **Windows Logon Security** (Sikkerhet på Windows-pålogging)—Beskytter Windows-kontoene dine ved å kreve bruk av HP Client Security-legitimering for tilgang.
   - **Pre-Boot Security (Power-on authentication)** (Sikkerhet før oppstart [Godkjenning når strømmen slås på])—Beskytter datamaskinen din før Windows starter opp. Dette valget er ikke tilgjengelig hvis BIOSen ikke støtter det.
   - **Allow One Step logon** (Tillat pålogging med ett trinn)—Denne innstillingen lar deg hoppe over påloggingen til Windows hvis godkjenning tidligere ble fullført ved oppstart eller Drive Encryption-nivå.

4. Klikk eller trykk **Users**, og klikk eller trykk på brukerens flis.

Brukere

Du kan overvåke og administrere denne datamaskinens HP Client Security-brukere.

For å legge til enda en Windows-brukeren til HP Client Security:

1. Fra Hjem-siden til HP Client Security klikker eller trykker du på **tannhjul**-ikonet.
2. På siden Avanserte innstillinger klikker eller trykker du på **Users** (Brukere).
3. Klikk eller trykk **Add another Windows user to HP Client Security** (Legg til enda en Windows-bruker til HP Client Security).
4. Skriv inn navnet til brukeren du vil legge til, og klikk eller trykk på **OK**.
5. Skriv inn brukerens Windows-passord.

   En flis for brukeren vises på Bruker-siden.

For å slette en Windows-brukeren fra HP Client Security:

1. Fra Hjem-siden til HP Client Security klikker eller trykker du på **tannhjul**-ikonet.
2. På siden Avanserte innstillinger klikker eller trykker du på **Users** (Brukere).
3. Klikk eller trykk på navnet til brukeren du vil slette.
4. Klikk eller trykk **Delete User** (Slett bruker), og klikk eller trykk **Yes** (Ja) for å bekrefte.

For å vise et sammendrag av policyene for pålogging og økter som håndheves for en bruker:

▲ Klikk eller trykk **Users** (Brukere), og klikk eller trykk på brukerens flis.

Mine policyer

Du kan vise din policyer for godkjenning og status for registrering. Mine policyer-siden har også koblinger til Policyer for administratorer og Policyer for vanlige brukere.

1. Fra Hjem-siden til HP Client Security klikker eller trykker du på **tannhjul**-ikonet.
2. På siden Avanserte innstillinger klikker eller trykker du på **My Policies** (Mine policyer).

   Policyer for pålogging og økter håndhevd for den nåværende påloggede brukeren vises.

Mine policyer-siden har også koblinger til Policyer for administrator på side 25 og Policyer for vanlige brukere på side 26.

Sikkerhetskopiere og gjenopprette dataen din

Det anbefales at du sikkerhetskopierer dataen til HP Client Security regelmessig. Hvor ofte du bør ta sikkerhetskopi, avhenger av hvor ofte dataen endres. Legger du eksempelvis til nye påloginger på daglig basis, bør du også ta sikkerhetskopi på daglig basis.

Sikkerhetskopier kan også brukes til å migrere fra én datamaskin til en annen, noe som også kalles importering og eksportering.

MERK: Bare Password Manager sikkerhetskopieres av denne funksjonen. Drive Encryption har en uavhengig metode for sikkerhetskopiering. Device Access Manager og informasjon om fingeravtrykk sikkerhetskopieres ikke.

HP Client Security må være installert på en datamaskin som skal motta den sikkerhetskopierte dataen før dataen fra sikkerhetskopifilen kan gjenopprettes.

For å sikkerhetskopierer dataen din:

1. Fra Hjem-siden til HP Client Security klikker eller trykker du på **tannhjul**-ikonet.
2. På siden Avanserte innstillinger klikker eller trykker du på **Administrator Policies** (Policyer for administratorer).
3. Klikk eller trykk på **Backup and Restore** (Sikkerhetskopier og gjenopprett).
4. Klikk eller trykk på **Backup** (Sikkerhetskopi), og verifiser deretter identiteten din.
5. Velg modulen du vil inkludere i sikkerhetskopien, og klikk eller trykk **Next** (Neste).
6. Skriv inn et navn for filen som lagres. Som standard lagres filen i Dokumenter-mappen din. For å spesifisere en annen lokasjon, klikk eller trykk på **Browse** (Bla gjennom).
7. Skriv inn og bekreft et passord for å beskytte filen.
8. Klikk eller trykk på **Save** (Lagre).

For å gjenopprette dataen din:

1. Fra Hjem-siden til HP Client Security klikker eller trykker du på **tannhjul**-ikonet.
2. På siden Avanserte innstillinger klikker eller trykker du på **Administrator Policies** (Policyer for administratorer).
3. Klikk eller trykk på **Backup and Restore** (Sikkerhetskopier og gjenopprett).
4. Velg **Restore** (Gjenopprett), og verifiser identiteten din.
5. Velg den tidligere filen du opprettet. Angi banen i det angitte feltet. For å spesifisere en annen lokasjon, klikk eller trykk på **Browse** (Bla gjennom).
6. Skriv inn passordet som ble brukt til å beskytte filen, og klikk eller trykk på **Next** (Neste).
7. Velg modulene du ønsker å gjenopprette data for.
8. Klikk eller trykk på **Restore** (Gjenopprett).

5 HP Drive Encryption (kun på enkelte modeller)

HP Drive Encryption gir deg fullstendig databeskyttelse ved å kryptere dataen til datamaskinen. Når Drive Encryption (stasjonskryptering) er aktivert, må du logge deg på Drive Encryption-påloggingsbildet, som vises før Windows®-operativsystemet starter.

HP Client Security Home-skjermen lar Windows-administratorer aktivere Drive Encryption, ta sikkerhetskopi av krypteringsnøkkelen og velge stasjon(er) eller partisjon(er) for kryptering. For mer informasjon, se programvarehjelpen i HP Client Security.

Følgende oppgaver kan utføres med Drive Encryption:

- Velge innstillinger for Drive Encryption:
  - Kryptere eller dekryptere individuelle stasjoner eller partisjoner med programvarekryptering
  - Kryptere eller dekryptere individuelle, selvkrypterende stasjoner med maskinvarekryptering
  - Legge til ekstra sikkerhet ved å deaktivere hvilemodus eller ventemodus, for å sikre at Drive Encryption alltid ber om godkjenning før oppstart

MERK: Kun interne SATA- og eksterne eSATA-stasjoner kan krypteres.

- Lage sikkerhetskopier av nøkler
- Gjenopprette tilgang til en kryptert datamaskin ved hjelp av sikkerhetskopierte nøkler og HP SpareKey
- Aktivere Drive Encryptions godkjenning før oppstart med passord, registrert fingeravtrykk eller PIN for valgte smartkort

Åpne Drive Encryption

Administratorer får tilgang til Drive Encryption ved å åpne HP Client Security:

1. Fra startskjermen klikker eller trykker du på **HP Client Security**-appen (Windows 8).

   – eller –

   Fra Windows-skrivebordet dobbeltklikker eller dobbelttrykker du på **HP Client Security**-ikonet i systemstatusfeltet, som du finner helt til høyre på oppgavelinjen.

2. Klikk eller trykk på **Drive Encryption**-ikonet.

Generelle oppgaver

Aktivere Drive Encryption for vanlige harddisker

Vanlige harddisker krypteres med programvarekryptering. Følg disse trinnene for å kryptere en stasjon eller en partisjon på en stasjon:

1. Åpne **Drive Encryption**. Se Åpne Drive Encryption på side 29 for å få mer informasjon.
2. Velg avmerkingsboksen for stasjonen eller partisjonen du vil kryptere, og klikk eller trykk på **Backup Key** (Sikkerhetskopi av nøkkel).

MERK: For bedre sikkerhet, velg avmerkingsboksen **Disable sleep mode for increased security** (Deaktiver hvilemodus for økte sikkerhet). Når du deaktiverer hvilemodus, er det ingen risiko for at påloggingsinformasjonen brukt til å låse stasjonen lagres i minnet.

3. Velg én eller flere av alternativene for sikkerhetskopi, og klikk eller trykk på **Backup** (Sikkerhetskopi). Se Sikkerhetskopiering av krypteringsnøkler på side 33 for å få mer informasjon.
4. Du kan fortsette å arbeide mens krypteringsnøkkelen blir sikkerhetskopiert. Ikke start datamaskinen din på nytt.

MERK: Du bes om å starte maskinen på nytt. Etter at maskinen har startet på nytt vil Drive Encryptions skjerm før oppstart vises, som krever godkjenning før Windows starter.

Drive Encryption har blitt aktivert. Kryptering av den valgte partisjonen(e) på en stasjon kan ta mange timer, avhengig av antallet partisjoner og størrelsen på partisjonen(e).

For mer informasjon, se programvarehjelpen i HP Client Security.

Aktivere Drive Encryption for selvkrypterende harddisker

Selvkrypterende stasjoner som oppfyller Trusted Computing Groups OPAL-spesifikasjoner for selvkrypterende behandling av stasjon, kan krypteres enten med programvarekryptering eller maskinvarekryptering. Maskinvarekryptering er mye raskere enn programvarekryptering. Du kan imidlertid ikke velge hvilken partisjon på stasjonen du vil kryptere. Hele stasjonen, inkludert alle partisjonene, vil krypteres.

For å kryptere spesifikke partisjoner, må du bruke programvarekryptering. Sørg for å fjerne haken i avmerkingsboksen **Only allow hardware encryption for Self-Encrypting Drives (SEDs)** (Tillat kun maskinvarekryptering for selvkrypterende stasjoner (SEDer)).

Følg disse trinnene for å aktivere Drive Encryption for selvkrypterende stasjoner:

1. Åpne **Drive Encryption**. Se Åpne Drive Encryption på side 29 for å få mer informasjon.
2. Velg avmerkingsboksen for stasjonen du vil kryptere, og klikk eller trykk på **Backup Key** (Sikkerhetskopi av nøkkel).

MERK: For bedre sikkerhet, velg avmerkingsboksen **Disable sleep mode for increased security** (Deaktiver hvilemodus for økte sikkerhet). Når du deaktiverer hvilemodus, er det ingen risiko for at påloggingsinformasjonen brukt til å låse stasjonen lagres i minnet.

3. Velg én eller flere av alternativene for sikkerhetskopi, og klikk eller trykk på **Backup** (Sikkerhetskopi). Se Sikkerhetskopiering av krypteringsnøkler på side 33 for å få mer informasjon.
4. Du kan fortsette å arbeide mens krypteringsnøkkelen blir sikkerhetskopiert. Ikke start datamaskinen din på nytt.

MERK: For selvkrypterende stasjoner vil du bes om å slå av datamaskinen.

For mer informasjon, se programvarehjelpen i HP Client Security.

Deaktivere Drive Encryption

1. Åpne **Drive Encryption**. Se Åpne Drive Encryption på side 29 for å få mer informasjon.
2. Fjern haken i avmerkingsboksen for alle krypterte stasjoner, og klikk eller trykk på **Apply** (Bruk).

   Drive Encryption starter med å dekryptere stasjonene.

MERK: Hvis programvarekryptering ble brukt, starter dekrypteringen. Det kan ta mange timer, avhengig på størrelsen på parisjonen(e) på den krypterte stasjonen. Når dekrypteringen er fullført, er Drive Encryption deaktivert.

Hvis maskinvarekryptering ble brukt, vil stasjonen umiddelbart dekrypteres, og etter et par minutter vil Drive Encryption være deaktivert.

Når Drive Encryption er deaktivert, vil du bes om å slå av maskinen, hvis stasjonen var maskinvarekryptert, eller om å starte maskinen på nytt, hvis stasjonen var programvarekryptert.

Logge på etter at Drive Encryption er aktivert

Når du slår på datamaskinen etter at Drive Encryption er aktivert og brukerkontoen din er registrert, må du logge inn på Drive Encryptions påloggingsskjem:

MERK: Når maskinen våkner fra hvilemodus eller ventemodus, vises ikke Drive Encryptions godkjenning før oppstart for programvarekryptering eller maskinvarekryptering. Maskinvarekryptering tilbyr alternativet **Disable sleep mode for increased security** (Deaktiver hvilemodus for økte sikkerhet), som hindrer maskinen fra å gå i hvilemodus eller ventemodus.

Når maskinen våkner fra dvale, vises Drive Encryptions godkjenning før oppstart for både programvarekryptering og maskinvarekryptering.

MERK: Hvis Windows-administratoren har aktivert BIOS Pre-boot Security i HP Client Security, og hvis One-Step Logon (ett-trinns pålogging) er aktivert (aktivert som standard), kan du logge inn på datamaskinen umiddelbart etter at du er godkjent i BIOS før oppstart, uten å måtte godkjennes igjen på Drive Encryptions påloggingsskjerm.

Pålogging for én bruker:

- ▲ På **Logon** (Pålogging)-siden skriver du inn Windows-passordet ditt, smartkort PINen, SpareKey eller sveiper en registrert finger.

Pålogging for flere brukere:

1. På **Select user to logon** (Velg bruker som skal logges på)-siden velger du brukeren du vil logge på fra rullegardinlisten, og klikker eller trykker deretter på **Next** (Neste).
2. På **Logon** (Pålogging)-siden skriver du inn Windows-passordet ditt, smartkort PINen eller sveiper en registrert finger.

MERK: Følgende smartkort støttes:

Støttede smartkort

- Gemalto Cyberflex Access 64k V2c

MERK: Hvis gjenopprettingsnøkkelen brukes til å logge på Drive Encryption-påloggingsskjermen, må du også logge deg på i Windows for å få tilgang til brukerkontoer.

Kryptering av ekstra harddisker

Det anbefales at du bruker HP Drive Encryption til å beskytte dataen din ved å kryptere harddisken din. Etter aktivering, kan ekstra harddisker eller partisjoner du har opprettet krypteres ved å følge disse trinnene:

1. Åpne **Drive Encryption**. Se Åpne Drive Encryption på side 29 for å få mer informasjon.
2. For selvkrypterende stasjoner velger du partisjonene på stasjonen som skal krypteres.

   MERK: Dette gjelder også for et scenario med forskjellige stasjoner, der systemet har både én eller flere vanlige harddisker og én eller flere selvkrypterende harddisker.

– eller –

▲ For maskinvarekrypterte stasjoner velger du andre stasjoner du vil kryptere.

Avanserte oppgaver

Administrere kryptering av stasjon (administratoroppgave)

Administratorer kan bruke Drive Encryption til å se eller endre krypteringsstatusen (Ikke kryptert eller Kryptert) for alle harddiskene i datamaskinen.

- Hvis statusen er Aktivert, har Drive Encryption blitt aktivert og konfigurert. Stasjonen er i en av følgende tilstander:

Programvarekryptering

- Ikke kryptert
- Kryptert
- Krypterer
- Dekrypterer

Maskinvarekryptering

- Kryptert
- Ikke kryptert (for ekstra stasjoner)

Kryptere eller dekryptere individuelle partisjoner på stasjon (kun programvarekryptering)

Administratorer kan bruke Drive Encryption til å kryptere én eller flere partisjoner på en harddisk på datamaskinen, eller dekryptere partisjoner på en harddisk som allerede har blitt kryptert.

1. Åpne **Drive Encryption**. Se Åpne Drive Encryption på side 29 for å få mer informasjon.
2. Under **Drive Status** (Status på stasjon) haker du av eller fjerner haken i avmerkingsboksen ved siden av hver partisjon på harddisken du vil kryptere eller dekryptere, og klikker eller trykker deretter på **Apply** (Bruk).

MERK: Når en partisjon blir kryptert eller dekryptert, vil en fremdriftsindikator viser hvor mange prosent av partisjonen som har blitt kryptert.

MERK: Dynamiske partisjoner støttes ikke. Hvis en partisjon vises som tilgjengelig, men ikke kan krypteres når den velges, er partisjonen dynamisk. En dynamisk partisjon oppstår når en partisjon krympes for å lage en ny partisjon med Diskbehandling.

En advarsel vises hvis en partisjon vil konverteres til en dynamisk partisjon.

Diskbehandling

- **Nickname** (Kallenavn)—Du kan gi stasjonene eller partisjonene navn for enklere å identifisere dem.
- **Disconnected drives** (Frakoblede stasjoner)—Drive Encryption kan spore stasjoner som fjernes fra datamaskinen. En stasjon som fjernes fra datamaskinen flyttes automatisk over til listen over frakoblede stasjoner. Hvis stasjonen settes tilbake inn i systemet, vil den igjen dukke opp i listen over tilkoblede stasjoner.
- Hvis du ikke lenger trenger å spore eller administrere den frakoblede stasjonen, kan du fjerne den frakoblede stasjonen fra listen.
- Drive Encryption forblir aktivert til avmerkingsboksene for alle de tilkoblede stasjonene er uten en hake, og listen med frakoblede stasjoner er tom.

Sikkerhetskopiering og gjenoppretting (administratoroppgave)

Når Drive Encryption er aktivert, kan administratorer bruke Encryption Key Backup-pakken til å ta sikkerhetskopi av krypteringsnøkler til flyttbare medier og til å gjennomføre en gjenoppretting.

Sikkerhetskopiering av krypteringsnøkler

Administratorer kan sikkerhetskopiere krypteringsnøkkelen for en kryptert stasjon på en flyttbar lagringsenhet.

FORSIKTIG: Sørg for å ha lagringsenheten med sikkerhetskopien av krypteringsnøkkelen på et trygt sted, for hvis du glemmer passordet ditt, mister smartkortet ditt eller ikke har registrert et fingeravtrykk, gir denne enheten deg kun tilgang til datamaskinen. Lagringsstedet bør også vært sikkert, siden lagringsenheten gir tilgang til Windows.

1. Åpne **Drive Encryption**. Se Åpne Drive Encryption på side 29 for å få mer informasjon.
2. Velg avmerkingsboksen for en stasjon, og klikk eller trykk deretter på **Backup Key** (Sikkerhetskopi av nøkkel).

3. Under **Create HP Drive Encryption recovery key** (Opprett gjenopprettingsnøkkel for HP Drive Encryption) velger du ett eller flere av følgende alternativer:

   - **Removable Storage** (Flyttbar lagringsenhet)—Velg avmerkingsboksen og deretter lagringsenehten hvor krypteringsnøkkelen vil lagres.
   - **SkyDrive**—Velg avmerkingsboksen. Du må være koblet til Internett. Logg inn på Microsoft SkyDrive og klikk eller trykk på **Yes** (Ja).

   MERK: For å bruke HP Drive Encryption-nøkkelen som er sikkerhetskopiert og lagret på SkyDrive, må du laste ned den fra SkyDrive til en flyttbar lagringsenhet, og sette lagringsenheten inn i denne datamaskinen.

   - **TPM** (kun utvalgte modeller)—Lar deg gjenopprette dataen din med et TPM-passord.

   FORSIKTIG: Hvis TPM er slettet eller datamaskinen er skadet, vil du miste tilgang til sikkerhetskopien. Hvis denne fremgangsmåten er valgt, bør også en annen metode for sikkerhetskopiering velges.

4. Klikk eller trykk på **Backup** (Sikkerhetskopi).

   Krypteringsnøkkelen lagres på lagringsenheten du valgte.

Gjenopprette tilgang til en aktivert datamaskin ved hjelp av sikkerhetskopierte nøkler

Administratorer kan foreta en gjenoppretting med Drive Encryption-nøkkelen som er sikkerhetskopiert til en flyttbar lagringsenhet ved aktivering, eller ved å velge **Backup Key** (Sikkerhetskopi av nøkkel).

1. Sett inn den flyttbare lagringsenhet som inneholder den sikkerhetskopierte nøkkelen.
2. Slå datamaskinen på.
3. Når HP Drive Encryption-påloggingsboksen åpnes, klikk eller trykk på **Recovery** (Gjenoppretting).
4. Skriv inn filbanen eller navnet som inneholder den sikkerhetskopierte nøkkelen din, og klikk eller trykk på **Recovery** (Gjenoppretting).
5. Når boksen hvor du må bekrefte handlingen åpner seg, klikker eller trykker du på **OK**.

   Påloggingsskjermen for Windows vises.

MERK: Hvis gjenopprettingsnøkkelen brukes til å logge på Drive Encryption-påloggingsskjermen, må du også logge deg på i Windows for å få tilgang til brukerkontoer. Det anbefales på det sterkeste at du tilbakestiller passordet etter at du har foretatt en gjenoppretting.

Gjennomføre en gjenoppretting med HP SpareKey

SpareKey-gjenoppretting Drive Encryptions godkjenning før oppstart krever at du svarer riktig på sikkerhetsspørsmål før du får tilgang til datamaskinen. For mer informasjon om å sette opp gjenoppretting med SpareKey, se programvarehjelpen i HP Client Security.

For å utføre en gjenoppretting med HP SpareKey hvis du glemmer passordet:

1. Slå datamaskinen på.
2. Når HP Drive Encryption vises, kan du gå til Brukerinnlogging-siden.

3. Klikk på **SpareKey**.

MERK: Hvis din SpareKey ikke har blitt initialisert i HP Client Security, er ikke **SpareKey**-knappen tilgjengelig.

4. Skriv inn riktig svar på spørsmål som vises, og klikk deretter på **Logon**.

   Påloggingsskjermen for Windows vises.

MERK: Hvis SpareKey brukes til å logge på Drive Encryption-påloggingsskjermen, må du også logge deg på i Windows for å få tilgang til brukerkontoer. Det anbefales på det sterkeste at du tilbakestiller passordet etter at du har foretatt en gjenoppretting.

6 HP File Sanitizer (kun på enkelte modeller)

File Sanitizer lar deg enkelt makulere elementer (for eksempel: personlig informasjon eller filer, historisk eller nettrelatert data, eller andre datakomponenter) fra datamaskinens interne harddisk, og lar deg også periodisk bleke datamaskinens interne harddisk.

File Sanitizer kan ikke brukes til å rense eller bleke følgende typer stasjoner:

- SSD-stasjoner, inkludert RAID-volumer som omfatter en SSD-enhet
- Eksterne harddisker koblet til med USB-, Firewire- eller eSATA-grensesnittet

Hvis en makulering eller bleking forsøkes på en SSD-stasjon, vil du få opp en advarsel og operasjonen vil ikke gjennomføres.

Makulering

Makulering er ikke det samme som å slette noe på vanlige måte i Windows®. Når du makulerer et element ved hjelp File Sanitizer, overskrives filene med meningsløs data, noe som gjør det nesten umulig å hente frem de opprinnelige elementene. Når du sletter noe på vanlige måte i Windows, vil ofte filen (eller elementet) forbli intakt på harddisken eller i en tilstand som kan la en rekke programmer gjenopprette den.

Du kan planlegge et tidspunkt frem i tid for makulering, eller du kan manuelt aktivere en makulering ved å velge **File Sanitizer**-ikonet på HP Client Security Home-skjermen eller bruke **File Sanitizer**-ikonet på Windows-skrivebordet. For mer informasjon se Sette opp en planlagt makulering på side 38, Makulering med høyreklikk på side 40 eller Starte en makulering manuelt på side 40.

MERK: Filer med endelsen .dll vil bare makuleres og fjernes fra systemet hvis den har blitt flyttet til søppelkassen.

Bleking av ledig plass

Når du sletter et element i Windows, vil ikke innholdet til elementet slettes fullstendig fra harddisken din. Windows sletter bare referansen til elementet, eller dens plassering på harddisken. Innholdet i elementet vil fortsatt bli værende på harddisken frem til et annen element overskriver det samme området på harddisken med ny informasjon.

Bleking av ledig plass lar deg på en sikker måte skrive tilfeldig data over slettede elementer, noe som hindrer brukere fra å se det originale innholdet til slettede elementer.

MERK: Bleking av ledig plass gir ingen ekstra sikkerhet for elementer som allerede har blitt makulert.

Du kan planlegge et tidspunkt frem i tid for bleking av ledig plass, eller du kan manuelt aktivere en bleking av tidligere makulerte elementer ved å velge **File Sanitizer**-ikonet på HP Client Security Home-skjermen eller bruke **File Sanitizer**-ikonet på Windows-skrivebordet. For mer informasjon se Sette opp en plan for bleking av ledig plass på side 39, Starte en manuell bleking av ledig plass på side 41 eller Bruke File Sanitizer-ikonet på side 40.

Åpne File Sanitizer

1. Fra startskjermen klikker eller trykker du på **HP Client Security**-appen (Windows 8).

   – eller –

   Fra Windows-skrivebordet dobbeltklikker eller dobbelttrykker du på **HP Client Security**-ikonet i systemstatusfeltet, som du finner helt til høyre på oppgavelinjen.

2. Under **Data** klikker eller trykker du på **File Sanitizer**.

– eller –

▲ Dobbeltklikk eller dobbelttrykk på **File Sanitizer**-ikonet på Windows-skrivebordet.

– eller –

▲ Høyreklikk eller trykk og hold på **File Sanitizer**-ikonet på Windows-skrivebordet, og velg deretter **Åpne File Sanitizer**.

Installasjonsprosedyrene

Shredding (Makulering)—File Sanitizer sletter eller makulerer valgte kategorier med elementer på en sikker måte.

1. Under **Shredding** (Makulering) haker du av avmerkingsboksen for hver type filer du vil makulere, eller fjerner haken i avmerkingboksen hvis du ikke vil makulere de filene.

   - **Recycle Bin** (Søppelbøtte)—Makulerer alle elementene i søppelbøtten.
   - **Temporary system files** (Midlertidige systemfiler)—Makulerer alle filer i mappen med midlertidige systemfiler. Følgende variabler for miljø søkes gjennom i følgende rekkefølge, og den første banen som finnes anses som systemmappen:
     - TMP
     - TEMP
   - **Temporary Internet files** (Midlertidige Internett-filer)—Makulerer kopier av nettsider, bilder og media som er lagret av nettlesere for å raskere kunne åpne nettsider.
   - **Cookies** (Informasjonskapsler)—Makulerer alle filer lagret på datamaskinen av nettsider som inneholder preferanser, som påloggingsinformasjon.

2. For å starte makuleringen klikker eller trykker du på **Shred** (Makuler).

Bleaching (Bleking)—Skriver tilfeldig data til den ledige plassen for å hindre gjenoppretting av slettede elementer.

▲ For å starte blekingen klikker eller trykker du på **Bleach** (Blek).

File Sanitizer Options (Alternativer for File Sanitizer)—Velg avmerkingsboksen for å aktivere følgende alternativer, eller fjern haken i avmerkingsboksen for å deaktivere et alternativ:

- **Enable Desktop icon** (Aktiver skrivebordsikon)—Viser File Sanitizer-ikonet på Windows-skrivebordet.
- **Enable right-click** (Aktiver høyreklikk)—Lar deg høyreklikk eller trykke og holde på et element, og deretter velge **HP File Sanitizer – Shred** (HP File Sanitizer – Makuler).

- **Ask for Windows password before manual shredding** (Spør om Windows-passordet før manuell makulering)—Krever godkjenning med Windows-passordet før et element manuelt makuleres.
- **Shred Cookies and Temporary Internet Files on browser close** (Makuler informasjonskapsler og midlertidige Internett-filer når nettleseren lukkes)—Makulerer alle valgte nettrelaterte elementer, som nettleserens URL-historikk, når du lokker en nettleser.

Sette opp en planlagt makulering

Du kan sette opp et tidspunkt for når makuleringen automatisk skal gjennomføres, eller du kan velge å makulere elementer manuelt når som helst. Se Installasjonsprosedyrene på side 37 for å få mer informasjon.

1. Åpne File Sanitizer og klikk eller trykk deretter på **Settings** (Innstillinger).
2. For å planlegge et fremtidig tidspunkt for makulering av elementer, går du til **Shred Schedule** (Makuleringsplan) og velger **Never** (Aldri), **Once** (Én gang), **Daily** (Daglig), **Weekly** (Ukentlig) eller **Monthly** (Månedlig), og angir en dato og et tidspunkt:
   a. Klikk eller trykk på time, minutt eller AM/PM-feltet.
   b. Bla til ønsket verdi vises på det samme nivået som de andre feltene.
   c. Klikk eller trykk på det hvite området rundt feltet for tidsinnstillingene.
   d. Gjenta for hvert felt til ønsket plan har blitt valgt.
3. Følgende fire typer elementer er oppført:
   - **Recycle Bin** (Søppelbøtte)—Makulerer alle elementene i søppelbøtten.
   - **Temporary system files** (Midlertidige systemfiler)—Makulerer alle filer i mappen med midlertidige systemfiler. Følgende variabler for miljø søkes gjennom i følgende rekkefølge, og den første banen som finnes anses som systemmappen:
     - TMP
     - TEMP
   - **Temporary Internet files** (Midlertidige Internett-filer)—Makulerer kopier av nettsider, bilder og media som er lagret av nettlesere for å raskere kunne åpne nettsider.
   - **Cookies** (Informasjonskapsler)—Makulerer alle filer lagret på datamaskinen av nettsider som inneholder preferanser, som påloggingsinformasjon.

   Hvis avmerket vil disse elementene makuleres på det planlagte tidspunktet.
4. For å velge flere tilpassede elementer som skal makuleres:
   a. Under **Scheduled Shred List** (Planlagt makuleringsliste) klikker eller trykker du på **Add folder** (Legg til mappe), og deretter navigerer du til filen eller mappen.
   b. Klikk eller trykk **Open** (Åpne), og klikk eller trykk deretter på **OK**.

   For å fjerne et element fra den planlagte makuleringslisten, fjerner du haken i avmerkingsboksen for elementet.

Sette opp en plan for bleking av ledig plass

Bleking av ledig plass gir ingen ekstra sikkerhet for elementer som allerede har blitt makulert.

1. Åpne File Sanitizer og klikk eller trykk deretter på **Settings** (Innstillinger).
2. For å planlegge et fremtidig tidspunkt for bleking av harddisken din, går du til **Bleach Schedule** (Blekingsplan) og velger **Never** (Aldri), **Once** (Én gang), **Daily** (Daglig), **Weekly** (Ukentlig) eller **Monthly** (Månedlig), og angir en dato og et tidspunkt.
   a. Klikk eller trykk på time, minutt eller AM/PM-feltet.
   b. Bla til ønsket tid vises på det samme nivået som de andre feltene.
   c. Klikk eller trykk på det hvite området rundt feltet for tidsinnstillingene.
   d. Gjenta til ønsket plan har blitt valgt.

MERK: Bleking av ledig plass kan ta lang tid. Sørg for at maskinen din er koblet til strømnettet. Selv om blekingen av den ledige plassen foregår i bakgrunnen, kan den økte prosessorbruken påvirke ytelsen til datamaskinen din. Bleking av ledig plass kan utføres på kveldtid eller når maskinen ikke er i bruk.

Beskytte filer fra makulering

For å beskytte filer eller mapper fra makulering:

1. Åpne File Sanitizer og klikk eller trykk deretter på **Settings** (Innstillinger).
2. Under **Never Shred List** (Aldri makuler-listen) klikker eller trykker du på **Add folder** (Legg til mappe), og deretter navigerer du til filen eller mappen.
3. Klikk eller trykk **Open** (Åpne), og klikk eller trykk deretter på **OK**.

MERK: Filene på denne listen er beskyttet så lenge de blir værende på listen.

For å fjerne et element fra listen fjerner du haken i avmerkingsboksen for elementet.

Generelle oppgaver

Bruke File Sanitizer til å utføre forskjellige oppgaver:

- **Bruke File Sanitizer-ikonet til å starte en makulering**—Dra filer til **File Sanitizer**-ikonet på Windows-skrivebordet. For mer informasjon, se Bruke File Sanitizer-ikonet på side 40.
- **Makulere et spesifikt element eller alle valgte elementer manuelt**—Makuler elementer når som helst, uten å måtte vente på det planlagte tidspunktet. For mer informasjon, se Makulering med høyreklikk på side 40 eller Starte en makulering manuelt på side 40.
- **Aktivere bleking av ledig plass manuelt**—Aktiver bleking av ledig plass når som helst. For mer informasjon, se Starte en manuell bleking av ledig plass på side 41.
- **Se loggfilene**—Se loggfilene fra makulering og bleking av ledig plass, som inneholder eventuelle feil eller mislykkede operasjoner fra den siste operasjonen med makulering eller bleking av ledig plass. For mer informasjon, se Vise loggfilene på side 41.

MERK: Makulering eller bleking av ledig plass kan ta lang tid. Selv om makuleringen og blekingen av den ledige plassen foregår i bakgrunnen, kan den økte prosessorbruken påvirke ytelsen til datamaskinen din.

Bruke File Sanitizer-ikonet

⚠ **FORSIKTIG:** Makulerte aktiva kan ikke gjenopprettes. Vurder nøye hvilke elementer du velger for manuell makulering.

Når du starter en makulering manuelt, vil den standard makuleringslisten i File Sanitizer makuleres (se Installasjonsprosedyrene på side 37).

Du kan starte en makulering manuelt på følgende måter:

1. Åpne File Sanitizer (se Åpne File Sanitizer på side 37) og klikk eller trykk på **Shred** (Makuler).
2. Når boksen hvor du må bekrefte handlingen åpner seg, må du passe på at elementene du vil makulere er valgt, og deretter klikke eller trykke på **OK**.

– eller –

1. Høyreklikk eller trykk og hold på **File Sanitizer**-ikonet på Windows-skrivebordet, og klikk deretter **Makuler nå**.
2. Når boksen hvor du må bekrefte handlingen åpner seg, må du passe på at elementene du vil makulere er valgt, og deretter klikke eller trykke på **Shred** (Makuler).

Makulering med høyreklikk

⚠ **FORSIKTIG:** Makulerte aktiva kan ikke gjenopprettes. Vurder nøye hvilke elementer du velger for manuell makulering.

Hvis **Enable right-click shredding** (Aktiver makulering med høyreklikk) har blitt valgt i File Sanitizer, kan du makulere et element på følgende måter:

1. Naviger til dokumentet eller mappen du vil makulere.
2. Høyreklikk eller trykk og hold på filen eller mappen, og velg deretter **HP File Sanitizer – Shred** (HP File Sanitizer – Makuler).

Starte en makulering manuelt

⚠ **FORSIKTIG:** Makulerte aktiva kan ikke gjenopprettes. Vurder nøye hvilke elementer du velger for manuell makulering.

Når du starter en makulering manuelt, vil den standard makuleringslisten i File Sanitizer makuleres (se Installasjonsprosedyrene på side 37).

Du kan starte en makulering manuelt på følgende måter:

1. Åpne File Sanitizer (se Åpne File Sanitizer på side 37) og klikk eller trykk på **Shred** (Makuler).
2. Når boksen hvor du må bekrefte handlingen åpner seg, må du passe på at elementene du vil makulere er valgt, og deretter klikke eller trykke på **OK**.

– eller –

1. Høyreklikk eller trykk og hold på **File Sanitizer**-ikonet på Windows-skrivebordet, og klikk deretter **Makuler nå**.
2. Når boksen hvor du må bekrefte handlingen åpner seg, må du passe på at elementene du vil makulere er valgt, og deretter klikke eller trykke på **Shred** (Makuler).

Starte en manuell bleking av ledig plass

Når du starter en bleking manuelt, vil den standard makuleringslisten i File Sanitizer blekes (se Installasjonsprosedyrene på side 37).

Du kan starte en bleking manuelt på følgende måter:

1. Åpne File Sanitizer (se Åpne File Sanitizer på side 37) og klikk eller trykk på **Bleach** (Blek).
2. Når boksen hvor du må bekrefte handlingen åpner seg, klikker eller trykker du på **OK**.

– eller –

1. Høyreklikk eller trykk og hold på **File Sanitizer**-ikonet på Windows-skrivebordet, og klikk deretter **Blek nå**.
2. Når boksen hvor du må bekrefte handlingen åpner seg, klikker eller trykker du på **Bleach** (Blek).

Vise loggfilene

Hver gang en makulering eller bleking av ledig plass utføres, vil loggfiler med eventuelle feil eller mislykkede operasjoner genereres. Loggfilene oppdateres alltid i henhold til den siste makuleringen eller blekingen.

MERK: Filer som ble makulert eller bleket vises ikke i loggfilene.

Det lages én loggfil for makulering og en annen for bleking av ledig plass. Begge loggfilene finner du på harddisken i følgende mapper:

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

For 64-biters systemer finner du loggfilene på harddisken i følgende mapper:

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

7 HP Device Access Manager (bare på enkelte modeller)

HP Device Access Manager kontrollerer tilgangen til data ved å deaktivere enheter som overfører data.

MERK: Noen menneskelige grensesnitt/inndataenheter, som mus, tastatur, TouchPad og fingeravtrykkleser, kontrolleres ikke av Device Access Manager. Se Ikke administrerte enhetsklasser på side 45 for å få mer informasjon.

Windows®-operativsystemets administratorer bruker HP Device Access Manager til å kontrollere tilgang til enheter på et system og til å beskytte mot uatorisert tilgang:

- Enhetsprofiler opprettes for hver bruker, for å definere enhetene de har lov eller ikke lov til å benytte.
- Just In Time Authentication (JITA) lar forhåndsdefinerte brukere godkjenne seg selv for å få tilgang til CD/DVD-stasjoner og flyttbare stasjoner som ellers blir avvist.
- Administratorer og kjente brukere kan ekskluderes fra begrensningene for tilgang til enhetene som påføres av DeviceAccess Manager, ved at del legges til gruppen Device Administrators. Medlemskap i denne gruppen administreres ved hjelp av avanserte innstillinger.
- Enhetstilgang kan gis eller nektes på grunnlag av gruppemedlemskap eller for individuelle brukere.
- For enhetsklasser som f.eks. CD-ROM-stasjoner og DVD-stasjoner, kan lesing og skriving tillates eller nektes separat.

HP Device Access Manager konfigureres automatisk med følgende innstillinger når du fullfører installasjonsveiviseren til HP Client Security:

- Just In Time Authentication (JITA) for flyttbare medier er aktivert for administratorer og brukere.
- Policyene for enheter gir full tilgang til andre enheter.

Åpne Device Access Manager

1. Fra startskjermen klikker eller trykker du på **HP Client Security**-appen (Windows 8).

   – eller –

   Fra Windows-skrivebordet dobbeltklikker eller dobbelttrykker du på **HP Client Security**-ikonet i systemstatusfeltet, som du finner helt til høyre på oppgavelinjen.

2. Under **Device** (Enhet) klikker eller trykker du på **Device Premissions** (Enhetstillatelser).

   - Standardbrukere kan se sin gjeldende enhetstilgang (se Brukervisning på side 43).
   - Administratorer kan se og gjøre endringer på enhetstilgangen som er konfigurert for datamaskinen ved å klikke eller trykke **Change** (Endre), og deretter skrive inn administratorpassordet (se Systemvisning på side 43).

Brukervisning

Når **Device Permissions** (Enhetstillatelser) er valgt, vil brukervisningen velges. Avhengig av policyene, kan standardbrukere og administratorer se sin egen tilgang til enhetsklasser eller individuelle enheter på denne datamaskinen.

- **Current user** (Gjeldende bruker)—Navnet til brukeren som i øyeblikket er logget på vises.
- **Device Class** (Enhetsklasse)—Typene enheter vises.
- **Access** (Tilgang)—Din gjeldende konfigurerte tilgang til typer enheter eller spesifikke enheter vises.
- **Duration** (Varighet)—Tidsperioden for din tilgang til CD/DVD-ROM-stasjoner eller flyttbare diskstasjoner vises.
- **Settings** (Innstillinger)—Administratorer kan endre hvilke stasjoner som får tilgangen kontrollert med Device Access Manager.

Systemvisning

I systemvisningen kan administratorer tillate eller nekte tilgang til enheter på denne datamaskinen for brukergruppe eller administratorgruppe.

▲ Administratorer får tilgang til systemvisningen ved å klikke eller trykke på **Change** (Endre), skrive inn administratorpassordet og velge fra følgende alternativer:

- **Device Access Manager**—For å slå HP Device Access Manager med Just In Time Authentication på eller av, klikk eller trykk på **On** (På) eller **Off** (Av).
- **Users and groups on this PC** (Brukere og grupper på denne datamaskinen)—Viser Brukere- eller Administratorer-gruppen som har tilgang eller nektes tilgang til de valgte enhetsklassene.
- **Device Class** (Enhetsklasse)—Viser enhetsklassene og enhetene som er installert på systemet, eller som kanskje har blitt installert på systemet tidligere. For å utvide listen, klikk på ikonet **+**. Alle enheter som er koblet til datamaskinen vises, og Administratorer- og Brukere-gruppen er utvidet for å vise deres medlemskap. For å oppdatere listen med enheter, klikk på den runde pilen (oppdater)-ikonet.
  - Beskyttelse er vanligvis i bruk for en enhetsklasse. Hvis tilgang er satt til **Allow** (Tillat), vil den valgte brukeren eller gruppen få tilgang til alle enheter i den enhetsklassen.
  - Beskyttelse kan også være i bruk for bestemte enheter.
  - Konfigurer Just In Time Authentication (JITA), for å gi utvalgte brukere tilgang til DVD/CD-ROM-stasjoner eller flyttbare diskstasjoner ved at de godkjenner seg selv. Se Konfigurasjon av JITA på side 44 for å få mer informasjon.
  - Tillat eller nekt tilgang til andre enhetsklasse, som flyttbare medier (eksempelvis USB-flash-stasjoner), seriell- og parallellporter, Bluetooth®-enheter, modem, PCMCIA/ExpressCard-enheter, 1394-enheter fingeravtrykklesere og smartkortlesere. Hvis fingeravtrykkleser og smartkortleser nektes, kan du brukes til å godkjenne en bruker, men kan ikke brukes i selve økten.

    MERK: Hvis Bluetooth-enheter brukes til å godkjenne en bruker, må tilgangen til Bluetooth-enheten ikke være begrenset i Device Access Manager.

  - Når du velger en innstilling på gruppe- eller klassenivå, og du blir spurt om du vil bruke innstillingen på underordnede objekter:

    Yes (Ja)—Innstillingen vil spres til underordnede objekter.

No (Nei)—Innstillingen vil ikke spres til underordnede objekter.

- Noen enhetsklasser, som DVD og CD-ROM, kan i noen tilfeller kontrolleres ytterligere ved å tillate eller nekte tilgang separat for lese- og skriveoperasjoner.

MERK: Administratorgruppen kan ikke legges til brukerlisten.

- **Access** (Tilgang)—Klikk eller trykk på pil ned, og velg deretter en av de følgende tilgangstypene for å tillate eller nekte tilgang:
  - **Tillat – Full tilgang**
  - **Tillat – Kun lesetilgang**
  - **Allow – JITA Required** (Tillat – Krever JITA)—For mer informasjon, se Konfigurasjon av JITA på side 44.

    Hvis denne tilgangstypen velges, kan du under **Duration** (Varighet) klikke eller trykke på pil ned for å velge en tidsgrense.
  - **Nekt**
- **Duration** (Varighet)—Klikk eller trykk på pil ned for å velge en tidsperiode for tilgang til CD/DVD-ROM-stasjoner eller flyttbare diskstasjoner (se Konfigurasjon av JITA på side 44).

Konfigurasjon av JITA

Konfigurasjon av JITA lar administratoren se og endre listene med brukere og grupper som har tilgang til enheter med Just In Time Authentication (JITA).

JITA-akiverte brukere vil få tilgang til noen enheter hvor det har blitt laget policyer i **Device Class Configuration** om at bruken er begrenset.

JITA-perioden kan godkjennes for et gitt antall minutter eller i en ubegrenset periode. Ubegrensede brukere vil ha tilgang til enheter fra tidspunktet de godkjenner seg selv og til de logger av systemet.

Hvis brukeren er gitt en begrenset JITA-periode, vil brukeren spørres om tilgangen skal forlenges ett minutt før JIRA-perioden er over. Så snart brukeren logger seg av systemet, eller en annen bruker logger seg inn, vil JIRA-perioden utløpe. Den neste gang brukere logger seg på og prøver å få tilgang til en JIRA-aktivert enhet, vil brukeren måtte skrive inn brukernavn og passord.

JITA er tilgjengelig for følgende enhetsklasser:

- DVD/CD-ROM-stasjoner
- Flyttbare diskstasjoner

Opprette en JITA-policy for en bruker eller gruppe

Administratorer kan gi brukere eller grupper tilgang til enheter med Just In Time Authentication (JITA).

1. Åpne **Device Access Manager** og klikk eller trykk på **Change** (Endre).
2. Velg brukeren eller gruppe, og deretter, under **Access** (Tilgang) for enten **Removable Disk drives** (Flyttbare diskstasjoner) eller **DVD/CD-ROM drives** (DVD/CD-ROM-stasjoner), klikk eller trykk på pil ned og velg **Allow – JITA Required** (Tillat – Krever JITA).
3. Under **Duration** (Varighet) klikker eller trykker du på pil ned for å velge en tidsperiode for JITA-tilgang.

Brukeren må logge av og deretter logge på igjen for at de nye JITA-innstillingen skal bli tatt i bruk.

Deaktivere en JITA-policy for en bruker eller gruppe

Administratorer kan deaktivere tilgangen til enheter for bruker eller gruppe med Just In Time Authentication (JITA).

1. Åpne **Device Access Manager** og klikk eller trykk på **Change** (Endre).
2. Velg brukeren eller gruppe, og deretter, under **Access** (Tilgang) for enten **Removable Disk drives** (Flyttbare diskstasjoner) eller **DVD/CD-ROM drives** (DVD/CD-ROM-stasjoner), klikk eller trykk på pil ned og velg **Deny** (Nekt).

Når brukeren logger seg på og prøver å få tilgang til enheten, vil tilgang være nektet.

Innstillinger

Settings (Innstillinger) lar administratorer se og endre stasjoner som har tilgangen sin kontrollert av Device Access Manager.

MERK: Device Access Manager må være aktivert når listen med stasjonsbokstaver konfigureres (se Systemvisning på side 43).

Ikke administrerte enhetsklasser

HP Device Access Manager administrerer ikke følgende enhetsklasser:

- Inndata-/utdataenheter
  - CD-ROM
  - Diskstasjon
  - Diskettstasjon-kontroller (FDC)
  - Harddisk-kontroller (HDC)
  - Klasse med enheter for menneskelig grensesnitt (HID)
  - Infrarøde enheter for menneskelig grensesnitt
  - Mus
  - Serielle multiport
  - tastatur
  - Plug and play (PnP)-skrivere
  - Skriver
  - Skriveroppgradering
- av/på
  - Støtte for avansert strømstyring (APM)
  - Batteri
- Diverse
  - Datamaskin
  - Dekoder
  - Skjerm

- Intel® enhetlig displaydriver
- Legacard
- Mediedriver
- Medieveksler
- Minneteknologi
- Skjerm
- Multifunksjon
- Nettklient
- Net-tjeneste
- Net-overføring
- Prosessor
- SCSI-adapter
- Sikkerhetsakselerator
- Sikkerhetsenhet
- System
- Ukjent
- Volum
- Volum-bilde

8 HP Trust Circles

HP Trust Circles er et sikkerhetsprogram for filer og dokumenter, som kombinerer kryptering av mapper og filer med en praktisk mulighet til å dele dokumenter med en klarert sirkel. Programmet krypterer filer plassert i mapper spesifisert av brukeren, og beskytte dem innenfor en klarert sirkel. Når filene er beskyttet, kan de bare brukes og deles av medlemmer i den klarerte sirkelen. Hvis en beskyttet fil mottas av noen som ikke er medlem, vil filen forbli kryptert og personen får ikke tilgang til innholdet.

Åpne Trust Circles

1. På startskjermen klikker eller trykker du på **HP Client Security**-appen.

   – eller –

   Fra Windows-skrivebordet dobbeltklikker du på **HP Client Security**-ikonet i systemstatusfeltet, som du finner helt til høyre på oppgavelinjen.

2. Under **Data** klikker eller trykker du på **Trust Circles**.

Komme i gang

Det er to måter du kan sende e-postinvitasjoner og svare på e-postinvitasjoner:

- **Using Microsoft® Outlook** (Bruke Microsoft® Outlook)—Hvis du bruker Trust Circles med Microsoft Outlook automatiseres behandlingen av Trust Circle-invitasjoner og -responser fra andre Trust Circle-brukere.
- **Using Gmail, Yahoo, Outlook.com or other email services (SMTP)** (Bruke Gmail, Yahoo, Outlook.com eller annen e-posttjeneste (SMTP))—Når du skriver inn navnet ditt, e-postadressen din og passordet ditt, bruker Trust Circles e-posttjenesten din til å sende e-postinvitasjoner til medlemmer valgt til å bli med i den klarerte sirkel.

For å sette opp den grunnleggende profilen din:

1. Skriv inn navnet ditt og e-postadressen din, og klikk eller trykk på **Next** (Neste).

   Navnet er synlig for alle medlemmer som er invitert til å bli med i din klarerte sirkel. E-postadressen brukes for å sende, motta eller svare på invitasjoner.

2. Skriv inn passordet for e-postkontoen og klikk eller trykk på **Next** (Neste).

   En e-post sendes som en test, for å sikre at e-postinnstillingene er korrekte.

   MERK: Datamaskinen må være koblet til et nettverk.

3. I **Trust Circle Name** (Navn på klarert sirkel)-feltet skriver du inne et navn for den klarerte sirkelen, og deretter klikker eller trykker du på **Next** (Neste).

4. Legg til medlemmer og mapper, og klikk eller trykk på **Next** (Neste). Den klarerte sirkelen opprettes med alle mapper som ble valgt, og sender e-postinvitasjoner til alle medlemmene som ble valgt. Hvis, av en eller annen grunn, en invitasjon ikke kan sendes, vises en melding. Medlemmer kan inviteres igjen når som helst fra Trust Circle-visningen ved å klikke **Your Trust**

Circles (Dine klarerte sirkler) og deretter dobbeltklikke eller dobbelttrykke på den klarerte sirkelen. Se Trust Circles på side 48 for å få mer informasjon.

Trust Circles

Du kan opprette en klarert sirkel første gang du bruker programmet, etter at du har skrevet inn e-postadressen din, eller i Trust Circle-visningen:

▲ Fra Trust Circle-visningen klikker eller trykker du på **Create Trust Circle** (Opprett klarert sirkel, og skriver deretter inn et navn for sirkelen.

- For å legge til medlemmer i den klarerte sirkelen, klikk eller trykk på ikonet **M+** ved siden av **Members** (Medlemmer), og følg deretter instruksjonene på skjermen.
- For å legge til mapper i den klarerte sirkelen, klikk eller trykk på ikonet **M+** ved siden av **Folders** (Mapper), og følg deretter instruksjonene på skjermen.

Legge til mapper i en klarert sirkel

Legge til mapper i en ny klarert sirkel:

- Mens du oppretter en klarert sirkel, kan du legge til mapper ved å klikke eller trykke på ikonet **+** ved siden av **Folders** (Mapper), og deretter følger instruksjonene på skjermen.

  – eller –

- I Windows Explorer høyreklikker eller trykker og holder du på en mappe som ikke er en del av en klarert sirkel, velger **Trust Circle** og deretter **Create Trust Circle from Folder** (Opprett klarert sirkel fra mappe).

TIPS: Du kan velge én eller flere mapper.

Legge til mapper i en eksisterende klarert sirkel:

- Fra Trust Circle-visningen klikker du **Your Trust Circles** (Dine klarerte sirkler), dobbeltklikker eller dobbelttrykker på den eksisterende klarerte sirkelen for å vise gjeldende mapper, klikker eller trykker på ikonet **+** ved siden av **Folders** (Mapper) og følger instruksjonene på skjermen.

  – eller –

- I Windows Explorer høyreklikker eller trykker og holder du på en mappe som ikke er en del av en klarert sirkel, velger **Trust Circle** og deretter **Add to existing Trust Circle from Folder** (Legg til eksisterende klarert sirkel fra mappe).

TIPS: Du kan velge én eller flere mapper.

Når en mappe er lagt til en klarert sirkel, vil Trust Circles kryptere mappen og innholdet automatisk. Når alle filene er kryptert vil en melding vises. I tillegg vil en grønn hengelås vises på ikonet til alle krypterte mapper og filene i mappene, noe som indikerer at de er beskyttet.

Legge til medlemmer i en klarert sirkel

Tre trinn er nødvendig for å legge medlemmer til i en klarert sirkel:

1. **Invite** (Inviter)—Først inviterer eieren av den klarerte sirkelen medlemmene. E-posten med invitasjonen kan sendes til flere brukere eller distribusjonslister/-grupper.
2. **Accept** (Godta)—Mottakeren av invitasjonen velger om han/hun vil godta eller avslå. Hvis mottakeren av invitasjonen godtar, vil en e-post med svaret sendes til personen som sendte invitasjonen. Hvis invitasjonen er sendt til en gruppe, mottar hvert medlem en invitasjon og velger å godta eller avslå.
3. **Enroll** (Registrer)—Den som inviterte har en siste sjanse til å avgjøre om medlemmet skal legges til i den klarerte sirkelen. Hvis den som inviterte bestemmer seg for å registrere medlemmet, vil en e-post sendes til den inviterte for å informere om dette. Den som inviterte og den som ble invitert kan alternativt verifisere sikkerheten til invitasjonsprosessen. En bekreftelseskode vises for den som ble invitert, som må oppgis til den som inviterte over telefon. Når koden er bekreftet, vil den som inviterte kunne sende den endelige e-posten om registrering.

Legge medlemmer til i en ny klarert sirkel:

▲ Mens du oppretter en klarert sirkel, kan du legge til medlemmer ved å klikke eller trykke på ikonet **M+** ved siden av **Members** (Medlemmer), og deretter følger instruksjonene på skjermen.

- Hvis du bruker Outlook, velger du kontaktene dine fra adresseboken i Outlook og klikker deretter **OK**.
- Hvis du bruker en annen e-posttjeneste, legger du enten til nye e-postadresser manuelt til Trust Circle, eller du kan hente dem fra e-postadressen registrert på Trust Circle.

Legge medlemmer til i en eksisterende klarert sirkel:

▲ Fra Trust Circles-visningen klikker du **Your Trust Circles** (Dine klarerte sirkler), dobbeltklikker eller dobbelttrykker på den eksisterende klarerte sirkelen for å vise gjeldende medlemmer, klikker eller trykker på ikonet **M+** ved siden av **Members** (Medlemmer) og følger instruksjonene på skjermen.

- Hvis du bruker Outlook, velger du kontaktene dine fra adresseboken i Outlook og klikker deretter **OK**.
- Hvis du bruker en annen e-posttjeneste, legger du enten til nye e-postadresser manuelt til Trust Circle, eller du kan hente dem fra e-postadressen registrert på Trust Circle.

Legge til filer i en klarert sirkel

Du kan legge til filer i en klarert sirkel på en av følgende måter:

- Kopier eller flytt filen inn i en eksisterende mappe i en klarert sirkel.

  – eller –

- I Windows Explorer høyreklikker eller trykker og holder du på en fil som ikke er kryptert, velger **Trust Circle** og deretter **Encrypt** (Krypter). Du vil ble bedt om å velge den klarerte sirkelen hvor du vil at filen skal legges til.

TIPS: Du kan velge én eller flere filer.

Krypterte mapper

Alle medlemmer av en klarert sirkel kan se og redigere filer som tilhører den klarerte sirkelen.

MERK: Trust Circle Manager/Reader synkroniserer ikke filer mellom medlemmer.

Filene må være delt på eksisterende måter, for eksempel e-post, FTP eller i en nettsky. Filer kopiert til, flyttet til eller opprettet i en mappe som er i en klarert sirkel, beskyttes umiddelbart.

Fjerne mapper fra en klarert sirkel

Når du fjerner en mappe fra en klarert sirkel vil mappen og alt innholdet dekrypteres, noe som fjerner beskyttelsen.

- Fra Trust Circles-visningen klikker eller trykker du **Your Trust Circles** (Dine klarerte sirkler), dobbeltklikker eller dobbelttrykker på den eksisterende klarerte sirkelen for å vise gjeldende mapper, og deretter klikker eller trykker du på **søppelbøtte**-ikonet ved siden av den mappen.

  – eller –

- I Windows Explorer høyreklikker eller trykker og holder du på en mappe som er en del av en klarert sirkel, velger **Trust Circles** og deretter **Remove from Trust Circle** (Fjern fra klarert sirkel).

TIPS: Du kan velge én eller flere mapper.

Fjerne en fil fra en klarert sirkel

For å fjerne en fil fra en klarert sirkel, høyreklikker eller trykker og holder du på en fil som er kryptert i Windows Explorer, velger **Trust Circle** og **Decrypt File** (Dekrypter fil).

Fjerne medlemmer fra en klarert sirkel

Et medlem som har blitt fullt ut registrert, kan ikke fjernes fra en klarert sirkel. Et alternativ vil være å opprette en ny klarert sirkel med alle de andre medlemmene, flytte alle filer og mapper til den nye sirkelen og deretter slette den gamle sirkelen. Dette vil sikre at alle nye filer som medlemmet mottar ikke vil være tilgjengelig, men alt som har blitt delt tidligere vil være tilgjengelig for medlemmet i den gamle klarerte sirkelen.

Hvis et medlem ikke er fullstendig registrert (enten har medlemmet blitt invitert til å bli med i en klarert sirkel eller medlemmet har ikke godtatt invitasjonen til en klarert sirkel), kan du fjerne medlemmet fra sirkelen på en av følgende måter:

- Fra Trust Circle-visningen klikker eller trykker du på **Your Trust Circles** (Dine klarerte sirkler), og deretter dobbeltklikker eller dobbelttrykker du på den klarerte sirkelen for å vise listen med medlemmer. Klikk eller trykk på **søppelbøtte**-ikonet ved siden av navnet til medlemmet du vil fjerne.
- Fra Trust Circle-visningen klikker eller tapper du på **Members** (Medlemmer), og deretter dobbeltklikker eller dobbelttrykker du på medlemmet for å vise de klarerte sirklene de er medlemmer av. Klikk eller trykk på **søppelbøtte**-ikonet ved siden av en klarert sirkel for å fjerne medlemmet fra den sirkelen.

Slette en klarert sirkel

For å slette en klarert sirkel må du eie den.

▲ Fra Trust Circle-visningen klikker eller trykker du på **Your Trust Circles** (Dine klarerte sirkler), og klikker eller trykker på **søppelbøtte**-ikonet ved siden av den klarerte sirkelen du vil slette.

Dette fjerner den klarerte sirkelen fra siden, og sender en e-post til alle medlemmene av den klarerte sirkelen for å informere dem om at den klarerte sirkelen har blitt slettet. Filer eller mapper som var en del av den klarerte sirkelen, blir dekryptert.

Velge innstillinger

Fra Trust Circle-visningen klikker eller trykker du på **Preferences** (Innstillinger). Tre faner vises

- **Innstillinger for e-post**

Alternativ	Beskrivelse
Brukernavn	Brukernavnet som brukes i øyeblikket vises. For å endre det skriver du inn et nytt brukernavn i den samme tekstboksen. Endringer lagres automatisk.
E-postadresse	E-postkontoen som brukes i øyeblikket vises. For å endre den klikker eller trykker du på **Change Email Settings** (Endre innstillinger for e-post) og følger instruksjonene på skjermen.
Bekreftelse av nytt medlem	Velg fra følgende alternativ: ◦ **Confirm Automatically** (Bekreft automatisk)—Etter å ha mottatt en aksept fra personen(e) du har invitert, bekreftes de i den klarerte sirkelen uten at du må foreta deg noe, og en bekreftende e-post sendes til personen(e) som ble invitert. ◦ **Confirm Manually** (Bekreft manuelt)—Etter å ha mottatt en aksept fra personen(e) du har invitert, kreves det en manuell handling for å registrere de nye medlemmene i den klarerte sirkelen, og deretter vil en bekreftende e-post sendes til personen(e) som ble invitert. ◦ **Require Verification** (Krever godkjenning)—Etter å ha mottatt en aksept fra personen(e) som ble invitert, kreves en bekreftelseskode for å registrere personen(e) som ble invitert. Eieren av den klarerte sirkelen må kontakte personen(e) som ble invitert og få bekreftelseskoden fra dem. Etter at korrekt kode er skrivet inn, vil de bekreftende e-postene sendes.
Periodisk godkjenning	Periodisk godkjenning krever at brukeren skriver inn Windows-passord etter det spesifiserte tidsavbruddet (registrert i minutter), og også når sensitive operasjoner utføres. Denne innstillingen gjør at brukere kan slå godkjenningen på eller av.
Godkjenning ved tidsavbrudd	Velg den angitte tidsavbruddsperioden (registrert i minutter) før godkjenning er nødvendig.
Ikke vis bekreftende melding	Velg avmerkingsboksen for å deaktivere visning av den bekreftende meldingen, eller fjern haken i avmerkingsboksen for å vise den bekreftende meldingen.
Jeg vil gjerne bidra til å forbedre HP Trust Circle gjennom anonym brukersporing	Velg avmerkingsboksen for å delta i programmet, eller fjern haken i avmerkingsboksen hvis du ikke ønsker å delta.

- **Sikkerhetskopiering/gjenoppretting**

Alternativ	Beskrivelse
Sikkerhetskopiere	Kopierer din Trust Circle Manager/Reader-programdata (innstillinger og klarerte sirkler) til en sikkerhetskopifil. Dersom systemet skulle krasje eller en systemfeil oppstår, kan du bruke denne filen til å gjenopprette din nye installasjon av Trust Circles til tilstand som er lagret i filen. **MERK:** Bare din Trust Circle-programdata lagres (klarerte sirkler, innstillinger og medlemmer). De faktiske filene i de klarerte sirklene tas det ikke sikkerhetskopi av. Disse filene bør du ta sikkerhetskopi av separat. For å sikkerhetskopiere Trust Circle-innstillinger og -brukerdata: **1.** Klikk eller trykk på **Backup** (Sikkerhetskopi). **2.** Velg et filnavn og en mappe for sikkerhetskopien, og klikk eller trykk deretter på **Save** (Lagre). **3.** Skriv inn et passord, bekreft det og klikk eller trykk på **OK**. Dette passordet kreves for å gjenopprette denne filen.
Gjenoppretting	Gjenoppretter innstillingene og de klarerte sirklene fra en sikkerhetskopifil, vanligvis etter en systemkrasj eller migrering til en annen datamaskin. For å gjenopprette Trust Circle Managers innstillinger or brukerdata: **1.** Klikk eller trykk på **Restore** (Gjenopprett). **2.** Naviger til mappen og filnavnet til sikkerhetskopifilen, og klikk eller trykk deretter på **Open** (Åpne). **3.** Skriv inn passordet som du skrev inn da du utførte sikkerhetskopieringen.

- **About** (Om)—Trust Circle Manager/Reader-programvareversjonen vises. Koblinger vises som lar deg oppgradere Trust Circle Manager til Pro-versjonen eller for å vise HPs personvernerklæring.

9 Tyverigjenoppretting (kun på enkelte modeller)

Computrace (kjøpes separat) lar deg eksternt overvåke, administrere og spore datamaskinen.

Når den er aktivert, konfigureres CompuTrace fra Absolut Software Customer Center. Fra kundenundesenteret kan administratoren konfigurere Computrace slik at det overvåker eller administrerer datamaskinen. Hvis systemet går tapt eller stjeles, kan Computer Center bistå lokale myndigheterr med å finne og gjenopprette datamaskinen. Hvis den er konfigurert, kan Computrace fortsatt fungere, selv om harddisken slettes eller skiftes ut.

For å aktivere Computrace:

1. Koble til Internett.
2. Åpne HP Client Security. Se Åpne HP Client Security på side 9 for å få mer informasjon.
3. Klikk på **Theft Recovery**.
4. For å starte Computrace veiviseren for aktivering, klikk på **Get Started**.
5. Angi kontaktinformasjon og betalingsinformasjon for kredittkort, eller angi en forhåndsbetalt produktnøkkel.

Aktiveringsveiviseren behandler transaksjonen sikkert og stiller inn brukerkontoen din på nettstedet Absolute Software Customer Center. Når prosessen er ferdig, får du en bekreftelses-e-post som inneholder din kontoinformasjon for kundesenteret.

Hvis du tidligere har brukt aktiveringsveiviseren for CompuTrace og kundesenterkontoen allerede finnes, kan du kjøpe flere lisenser ved å kontakte din HP-kontorepresentant.

For å logge på kundesenteret:

1. Gå til https://cc.absolute.com/.
2. I feltene **Login ID** og **Password** skriver du inn påloggingsopplysnignene du fikk i bekreftelses-e-posten, før du klikker på **Logg på**.

Ved hjelp av kundesenteret kan du:

- Overvåke datamaskinene.
- Beskytte eksterne data.
- Melde fra om tyveri av alle datamaskiner som er beskyttet av Computrace.

▲ Klikk på **Learn More** hvis du vil ha mer informasjon om Computrace.

10 Lokaliserte passordunntak

På godkjenningsnivået når strømmen slås på og på HP Drive Encryption-nivået, er støtten for passordlokalisering begrenset. Se Windows IMEer støttes ikke på godkjenningsnivået når strømmen slås på eller på Drive Encryption-nivået på side 54 for å få mer informasjon.

Hva du må gjøre når et passord avvises

Passord kan bli avvist av følgende årsaker:

- En bruker har valgt å bruke en IME som ikke støttes. Dette er et vanlig problem med dobbel-byte-språk (koreansk, japansk, kinesisk). For å løse dette problemet:
  1. Bruk **Kontrollpanelet** til å legge til et støttet tastatur (legg til amerikansk/engelsk tastatur under kinesisk inndataspråk).
  2. Sett det støttede tastaturet som standard inndata.
  3. Åpne HP Client Security og skriv inn Windows-passordet.
- En bruker har valgt å bruke et tegn som ikke støttes. For å løse dette problemet:
  1. Endre Windows-passord slik at det bare bruker støttede tegn. For mer informasjon om tegn som ikke støttes, kan du se Håndtering av spesialtaster på side 55.
  2. Åpne HP Client Security og skriv inn Windows-passordet.

Windows IMEer støttes ikke på godkjenningsnivået når strømmen slås på eller på Drive Encryption-nivået

I Windows kan brukeren velge en IME (Input Method Editor) for å angi kompliserte tegn og symboler, for eksempel japanske eller kinesiske tegn, ved hjelp av et vanlig, vestlig tastatur.

IMEer støttes ikke på godkjenningsnivået når strømmen slås på eller på Drive Encryption-nivået. Et Windows-passord kan ikke skrives inn med en IME ved godkjenning når strømmen slås på eller på påloggingsskjermen til HP Drive Encryption, noe som kan føre til en situasjon der du blir låst ute. I noen tilfeller viser ikke Microsoft Windows® IME en når brukeren skriver inn passordet.

Løsningen er å bytte til et av følgende støttede tastaturoppsett, som oversetter til tastaturoppsett 00000411:

- Microsoft IME for japansk
- Den japanske tastaturoppsettet
- Office 2007 IME for japansk—Hvis Microsoft eller en tredjepart bruker uttrykket IME eller Input Method Editor, er det ikke sikkert inndatametoden faktisk er en IME. Dette kan føre til forvirring, men programvaren leser heksadesimalkoden. Så hvis en IME er tilknyttet et støttet tastaturoppsett, vil HP Client Security kunne støtte konfigurasjonen.

⚠ **ADVARSEL:** Når HP Client Security er distribuert, vil passord skrevet inn med en Windows IME bli avvist.

Passordendringer ved hjelp av tastaturoppsett som også støttes

Hvis passordet i utgangspunktet er satt med ett tastaturoppsett, for eksempel Amerikansk engelsk (409), og brukeren deretter endrer passordet ved hjelp av et annet tastaturoppsett som også støttes, for eksempel Latinamerikansk (080A), vil det endrede passordet fungere i HP Drive Encryption, men det vil ikke fungere i BIOS hvis brukeren bruker tegn som finnes i det sistnevnte oppsettet men ikke i det første (for eksempel ē).

MERK: Administratorer kan løse dette problemet ved å bruke HP Client Security Brukere-siden (som du får tilgang til fra **tannhjul**-ikonet på Hjem-siden) til å fjerne brukeren fra HP Client Security, velge ønsket tastaturoppsett i operativsystemet og deretter kjøre installasjonsveiviseren for HP Client Security på nytt for samme bruker. BIOS lagrer ønsket tastaturoppsett, og passordene som kan skrives inn med dette tastaturoppsettet vil settes på riktig måtte i BIOS.

Et annet potensielt problem er bruk av ulike tastaturoppsett som alle kan lage de samme tegnene. For eksempel kan både det internasjonale, amerikanske tastaturoppsettet (20409) og Latinamerikansk-tastaturoppsett (080A) produsere tegnet é, selv om ulike sekvenser med tastetrykk kan være nødvendig. Hvis et passord i utgangspunktet er satt med Latinamerikansk-tastaturoppsett, vil Latinamerikansk-tastaturoppsett settes i BIOS, selv om passordet senere endres ved bruk av det internasjonale, amerikanske tastaturoppsettet.

Håndtering av spesialtaster

- Kinesisk, slovakisk, kanadisk fransk og tsjekkisk

  Når en bruker velger en av de foregående tastaturoppsettene, og deretter angir et passord (for eksempel, abcdef), må det samme passordet angis mens skift-knappen holdes nede for liten bokstav, og shift-tasten og caps lock for store bokstaver i Power-on-godkjenning og HP Drive-kryptering. Numeriske passord må være angitt ved hjelp av det numeriske tastaturet.

- Koreansk

  Når en bruker velger et støttet koreansk tastaturoppsett og deretter angir et passord (for eksempel, abcdef), må det samme passordet angis mens høyre alt-tasten holdes nede for liten bokstav, og høyre alt-tasten og caps lock for store bokstaver i Power-on-godkjenning og HP Drive-kryptering.

- Tegn som ikke støttes er oppført i den påfølgende tabellen:

Language (språk)	Windows	BIOS	Drive Encryption
Arabisk	ﻷ ,ﻹ og ﻵ-tastene genererer to tegn.	ﻷ ,ﻹ og ﻵ-tastene genererer ett tegn.	ﻷ ,ﻹ og ﻵ-tastene genererer ett tegn.
Fransk (Canada)	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 Power On-godkjenning.	Ç, è, à, og é med caps lock er ç, è, à, og é i HP Drive Encryption.

Language (språk)	Windows	BIOS	Drive Encryption
Spansk	40a støttes ikke. Det fungerer likevel fordi programvaren konverterer det til c0a. Men på grunn av subtile forskjeller mellom tastaturoppsettene, anbefales det at spansktalende brukere endrer Windows-tastaturoppsettet til 1040a (spansk variasjon) eller 080a (Latinamerikansk).	n/a	n/a
Internasjonal amerikansk	◦ ¡, ¤, ‘, ’, ¥ og ×-tastene på den øverste raden avvises. ◦ å, ® og Þ-tastene på den andre raden avvises. ◦ á, ð og ø-tastene på den tredje raden avvises. ◦ æ-tasten på den nederste raden avvises.	n/a	n/a
Tsjekkisk	◦ ğ-tasten avvises. ◦ į-tasten avvises. ◦ ų-tasten avvises. ◦ ė, ı og ż-tastene avvises. ◦ ģ, ķ, ļ, ņ og ţ-tastene avvises.	n/a	n/a
Slovakisk	ż-tasten avvises.	◦ š, ś og ş-tastene avvises når de skrives inn, men godtas når de skrives inn med et programvaretastatur. ◦ ţ-dødtasten genererer to tegn.	n/a
Ungarsk	ż-tasten avvises.	ţ-tasten genererer to tegn.	n/a
Slovensk	żŻ-tasten avvises i Windows, og alt-tasten genererer en dødtast i BIOS.	ú, Ú, ů, Ů, ş, Ş, ś, Ś, š og Š-tastene avvises i BIOS.	n/a
Japansk	Når tilgjengelig er Microsoft Office 2007 IME et bedre valg. Til tross for IME-navnet, er det faktisk tastaturoppsett 411 som støttes.	n/a	n/a

Ordliste

administrator-
Se *Windows-administrator*.

aktiva
En datakomponent som består av personlig informasjon eller filer, historisk og nettrelatert data, osv., som er plassert på harddisken.

aktivering
Oppgaven som må være fullført før noen av Drive Encryption-funksjonene er tilgjengelige. Administratorer kan aktivere Drive Encryption med HP Client Security-installasjonsveiviseren eller HP Client Security. Aktiveringsprosessen består av å aktivere programvaren, kryptere harddisken og opprette den første sikkerhetskopien av nøkkelen på en flyttbar lagringsenhet.

autentisering
Prosess for å bekrefte at du er den personen du hevder å være, gjennom bruk av legitimasjon, inkludert Windows-passordet, fingeravtrykk, et smartkort, et kontaktfritt kort eller et nærhetskort.

autentisering ved oppstart
En sikkerhetsfunksjon som krever en form for godkjenning, for eksempel et smartkort, sikkerhetsbrikke eller passord, når datamaskinen blir slått på.

automatisk makulering
Makulering som du planlegger i File Sanitizer.

bleking av ledig plass
Skriving av tilfeldig data over slettede elementer og ubrukt plass. Denne prosessen reduserer eksistensen til slettede elementer, så de originale elementene er vanskeligere å gjenopprette.

Bluetooth-
Teknologi som bruker radiooverføring til å aktivere Bluetooth-aktiverte datamaskiner, skrivere, mus, mobiltelefoner og andre enheter med trådløs kommunikasjon over kort avstand.

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

dekryptering
En prosedyre som brukes i kryptografi for å konvertere kryptert data til ren tekst.

domene
En gruppe datamaskiner som er en del av et nettverk og har felles katalogdatabase. Domenene har unike navn, og hvert domene har et felles sett med regler og prosedyrer.

Drive Encryption
Beskytter data ved å kryptere harddisker, slik at data blir uleselige for alle uten riktig godkjenning.

Drive Encryption-påloggingsbilde (Stasjonskryptering)
Se Drive Encryptions godkjenning før oppstart.

Drive Encryptions godkjenning før oppstart
En påloggingsskjerm som vises før Windows starter. Brukerne må skrive inn Windows-brukernavnet og passord eller smartkort-PIN, eller sveipe en registrert finger. Hvis ett-trinns pålogging er valgt, vil du ved å skrive inn

riktig informasjon på Drive Encryption-påloggingsskjermen få direkte tilgang til Windows, uten å måtte logge deg på igjen på Windows-påloggingsskjermen.

DriveLock-
En sikkerhetsfunksjon som kobler harddisken til en bruker og krever at brukeren angir riktig DriveLock-pasord når datamaskinen startes.

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

enhetsklasse
Alle enheter av en gitt type, som stasjoner.

fingeravtrykks
En digital ekstraksjon av fingeravtrykket ditt. Bildet av ditt faktiske fingeravtrykk lagres aldri av HP Client Security.

gjenoppretting
En prosess som kopierer programinformasjon fra en tidligere lagret sikkerhetskopifil inn i programmet.

Gjenoppretting med HP SpareKey
Muligheten til å få tilgang til datamaskinen ved å oppgi riktig svar på sikkerhetsspørsmål.

gruppe
En gruppe brukere som har det samme nivået med tilgang/ikke tilgang til en enhetsklasse eller en spesifikk enhet.

Hjemmeside
Et sentralt sted hvor du kan få tilgang til og administrere funksjonene og innstillingene i HP Client Security.

identitet
I HP Client Security, en gruppe påloggingsopplysninger og innstillinger som håndteres som en konto eller profil for en bestemt bruker.

ID-kort
En applikasjon på Windows-skrivebordet som visuelt identifiserer datamaskinen din, med brukernavn og valgt bilde.

Just In Time Authentication
Se programvarehjelpen for HP Device Access Manager.

katastrofegjenopprettingsarkiv
Et beskyttet lagringsområde som gjør det mulig å kryptere grunnleggende brukernøkler mellom ulike plattformeiernøkler.

Klarert sirkel
Begrenser tilgangen til data ved å binde den opp til definerte grupper med klarerte brukere. Dette forhindrer at dataen havner i feil hender, enten ved et uhell eller med vilje. Dataen er sikret med CryptoMills Zero Overhead Key Management-teknologi og kryptert, så bare den klarerte sirkelen får tilgang til den. Dette forhindrer dekryptering av dokumenter eller andre sensitive opplysninger utenfor den klarerte sirkelen

kontaktfritt kort
Et plastkort som inneholder en databrikke som kan brukes til godkjenning.

kryptering
En prosedyre, for eksempel bruk av en algoritme, som brukes i kryptografi for å konvertere vanlig tekst til chiffertekst,, for å forhindre at uautoriserte mottakere leser informasjonen. Det finnes mange typer datakryptering, og de er grunnlaget for nettverkssikkerhet. Vanlige typer er Data Encryption Standard og kryptering av fellesnøkler.

makulere

Utførelsen av en algoritme som overskriver dataen i et element med meningsløs data.

manuell makulering
Umiddelbar makulering av et element eller valgte elementer, som gjennomføres uavhengig av planlagte makuleringer.

Mappe i klarert sirkel
En mappe som er beskyttet av en klarert sirkel.

maskinvarekryptering
Bruk av selvkrypterende stasjoner er i henhold til Trusted Computing Groups OPAL-spesifikasjoner for selvkrypterende behandling av stasjonen, og kan fullføre umiddelbar kryptering. Maskinvarekryptering er umiddelbar og tar bare noen få minutter, mens programvarekryptering kan ta mange timer.

nettverkskonto
Windows-bruker eller administratorkontoen, enten på en lokal datamaskin, i en arbeidsgruppe, eller på et domene.

nærhetskort
Et plastkort som inneholder en databrikke som kan brukes til godkjenning i forbindelse med annen legitimasjons, for ekstra sikkerhet.

omstart
Omstart av datamaskinen.

PIN-kode
Et personlig ID-nummer for en registrert bruker som brukes i forbindelse med godkjenning.

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

policy for kontroll over enhetstilgang
Listen med enheter som en bruker har tilgang til eller nektes tilgang til.

programvarekryptering
Bruk av programvare til å kryptere harddisken, sektor etter sektor. Denne prosessen er tregere enn maskinvarekryptering

pålogging
Et objekt i HP Client Security som består av et brukernavn og passord (og muligens annen valgt informasjon) som kan brukes til å logge på nettsteder eller andre programmer.

påloggingsinformasjon
Spesifikk informasjon eller en maskinvareenhet som brukes til å godkjenne deg som en individuell bruker.

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

sikkerhetspåloggingsmetode
Metoden du bruker til å logge deg på datamaskinen.

Single Sign On (Engangspålogging)
En funksjon som lagrer godkjenningsinformasjon og gjør at du kan bruke HP Client Security for å få tilgang til Internett og Windows-programmer som krever passordgodkjenning.

smartkort
En maskinvareenhet som kan brukes med en PIN-kode for godkjenning.

Tilkoblet enhet

En maskinvareenhet som er koblet til en port på datamaskinen.

Trust Circle Manager/Reader
Trust Circle Reader kan bare godta invitasjoner sendt ut av Trust Circle Manager-brukere. Trust Circle Manager lar deg imidlertid opprette klarerte sirkler. Funksjoner inkluderer invitasjon av personer via e-post til en klarert sirkel og aksept av invitasjoner til klarerte sirkler fra andre. Når en klarert sirkel er opprettet, kan filer beskyttet av den klarerte sirkelen deles på en sikker måte.

Trusted Platform Module (TPM) innebygd sikkerhetsbrikke
En tredjeparts vedlikeholdsleverandør godkjenner en datamaskin, i stedet for en bruker, ved å lagre informasjon som er spesifikk for vertssystemet, for eksempel krypteringsnøkler, digitale sertifikater og passord. En tredjeparts vedlikeholdsleverandør minimerer risikoen for at informasjon på datamaskinen kompromitteres av fysisk tyveri eller av en ekstern hacker.

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

Windows-brukerkonto
En bruker som er autorisert til å logge seg på et nettverk eller på en enkelt datamaskin.

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

Stikkordregister