Hjemmeside for Dell Data Protection | Access

Hjemmesiden for **Dell Data Protection | Access** er startstedet for tilgang til funksjonene i dette programmet. Du kan få tilgang til følgende fra dette vinduet:

System Access Wizard
Tilgangsalternativer
Self-Encrypting Drive
Avanserte alternativer

I nederste høyre hjørne i vinduet finner du en kobling kalt **avansert**, som du kan klikke på for å få tilgang til avanserte alternativer.

I avanserte alternativer kan du klikke på **hjem**-koblingen nederst til høyre i vinduet for å gå tilbake til hjemmesiden.

System Access Wizard

System Access Wizard startes automatisk første gang programmet **Dell Data Protection | Access** startes. Denne veiviseren går gjennom konfigurering av alle sider ved sikkerheten i systemet, Inkludert hvordan (for eksempel bare passord eller fingeravtrykk og passord) og når (ved Windows-pålogging, pre-Windows-pålogging eller begge) du vil logge på systemet. Hvis systemet har en selvkrypterende stasjon, kan du også konfigurere denne via veiviseren.

Administratorfunksjoner

Brukere som er konfigurert med administratorrettigheter for Windows i systemet, har rett til å utføre følgende funksjoner i **Dell Data Access | Protection** som standardbrukere ikke kan utføre:

- Angi/endre systempassord (pre-Windows-passord)
- Angi/endre harddiskpassord
- Angi/endre administratorpassord
- Angi/endre TPM-eierpassord
- Angi/endre ControlVault-administratorpassord
- Tilbakestille system
- Arkivere og gjenopprette legitimasjoner
- Angi/endre administrator-PIN-kode for smartkort
- Fjerne/tilbakestille et smartkort
- Aktivere/deaktivere sikker Dell-pålogging til Windows
- Angi policy for Windows-pålogging
- Administrere selvkrypterende stasjoner, inkludert
    - Aktivere/deaktivere låsing av selvkrypterende stasjoner
    - Aktivere/deaktivere synkronisering med Windows-passord (WPS)
    - Aktivere/deaktivere Single Sign On (SSO)
    - Utføre en kryptografisk sletting

Fjernadministrasjon

En organisasjon kan konfigurere et miljø der sikkerhetsfunksjonene i programmet **Dell Data Protection | Access** på flere plattformer behandles sentralt (det vil si fjernadministrasjon). I dette tilfellet kan infrastrukturen for Windows-sikkerhet, som Active Directory, brukes til sikker behandling av bestemte funksjoner i **Dell Data Protection | Access**.

Når en datamaskin administreres eksternt (for eksempel "eies" av den eksterne administratoren), deaktiveres lokal administrasjon av funksjonene i **Dell Data Protection | Access**. Vinduene for behandling av funksjonene vil ikke være tilgjengelig lokalt. Følgende funksjoner kan behandles eksternt:

- Trusted Platform Module (TPM)
- ControlVault
- Pre-Windows-pålogging
- Tilbakestill system
- BIOS-passord
- Policy for Windows-pålogging
- Self-Encrypting Drive-enheter
- Registrering av fingeravtrykk og smartkort

Hvis du vil ha mer informasjon om Wave Systems' EMBASSY® Remote Administration Server (ERAS) for ekstern administrasjon, kan du kontakte en Dell-selger eller gå til dell.com.

Tilgangsalternativer

Fra vinduet Tilgangsalternativer kan du angi hvordan du skal få tilgang til systemet.

Hvis du har konfigurert alternativer for **Dell Data Protection | Access**, vises disse på hjemmesiden med de tilgjengelige alternativene (for eksempel endre passord for pre-Windows-pålogging). De tilgjengelige alternativene er snarveier som du kan klikke på for å komme til det riktige vinduet for å utføre en bestemt oppgave (for eksempel å endre pre-Windows-passordet eller registrere et nytt fingeravtrykk).

Generelt
Først kan du angi når du skal logge deg på (Windows-pålogging, pre-Windows-pålogging eller begge) og hvordan (for eksempel fingeravtrykk og passord) du skal logge deg på. Du kan velge ett eller to alternativer for pålogging, og disse inkluderer kombinasjoner av fingeravtrykk, smartkort og passord. De oppførte alternativene baseres på påloggingspolicyer i miljøet og hva som støttes på plattformen.

Fingeravtrykk
Hvis systemet inneholde en fingeravtrykkleser, kan du registrere eller oppdatere fingeravtrykk for bruk ved pålogging til systemet. Når du har registrert fingeravtrykk, kan du dra den eller de registrerte fingrene på systemets fingeravtrykkleser for å få tilgang til systemet ved Windows-pålogging, pre-Windows-pålogging eller begge (avhengig av hva du har angitt i de generelle tilgangsalternativene). Se Registrere fingeravtrykk for brukere hvis du vil ha mer informasjon.

Pre-Windows-pålogging
Hvis du har angitt at brukere må logge seg på med pre-Windows-pålogging, må du konfigurere et systempassord (også kalt pre-Windows-passordet) for pre-Windows-tilgang. Etter at dette er konfigurert, kan administratoren når som helst endre passordet.

Du kan også deaktivere pre-Windows-pålogging fra dette skjermbildet. For å gjøre det må du oppgi det gjeldende systempassordet, bekrefte at passordet er riktig, og deretter klikke på **Deaktiver**-knappen.

Smartkort
Hvis du har angitt at brukere må bruke et smartkort for å logge seg på, må du registrere ett eller flere vanlige (som må være i kontakt) smartkort eller smartkort uten kontakt. Klikk på koblingen **Registrer et annet smartkort** for å starte veiviseren for registrering av smartkort. Å registrere smartkortet betyr å konfigurere pålogging ved bruk av kortet.

Når du har registrert et smartkort, kan du endre eller konfigurere en PIN-kode for kortet via koblingen **Endre eller konfigurer smartkort-PIN-kode**.

Pre-Windows-pålogging

Når vinduet Pre-Windows-pålogging er konfigurert, må du gi godkjenning (passord, fingeravtrykk eller smartkort) når systemet slås på, før Windows lastes inn. Funksjonen Pre-Windows-pålogging gir ekstra sikkerhet til systemet og hindrer at uautoriserte brukere får tilgang til Windows og datamaskinen (for eksempel hvis den blir stjålet).

Fra vinduet Pre-Windows-pålogging kan administratorer konfigurere pre-Windows-pålogging eller opprette eller endre et pre-Windows-passord (systempassord). Hvis det allerede er konfigurert et slik passord, kan du deaktivere pre-Windows-pålogging fra dette vinduet. Ved konfigurasjon av pre-Windows-pålogging startes det en veiviser der du kan gjøre følgende:

- Systempassord: Konfigurere et systempassord (også kalt et pre-Windows-passord) for pre-Windows-tilgang. Dette passordet kan også brukes som en reserveløsning i tilfeller der en bruker har andre godkjenningsfaktorer (for eksempel for å få tilgang til systemet hvis det er problemer med fingeravtrykksføleren).
- Fingeravtrykk eller smartkort: Konfigurere et fingeravtrykk eller smartkort for bruk ved pre-Windows-pålogging, og angi om denne godkjenningsfaktoren skal brukes i stedet for, eller i tillegg til, pre-Windows-passordet.
- Single Sign On: Pre-Windows-godkjenning (passord, fingeravtrykk eller smartkort) vil som standard brukes til å automatisk logge deg på Windows også (dette kalles Single Sign On). Hvis du vil deaktivere denne funksjonen, merker du av for Jeg vil logge på på nytt til Windows.
- Hvis det er angitt et BIOS-harddiskpassord i tillegg til et pre-Windows-passord, kan du også endre eller deaktivere harddiskpassordet.

MERK: Enkelte fingeravtrykkslesere er ikke aktivert for bruk ved pre-Windows-godkjenning. Hvis leseren ikke er kompatibel, kan du registrere fingeravtrykk bare for Windows-pålogging. Kontakt systemadministrator for å få vite om en bestemt fingeravtrykksleser er kompatibel, eller gå til support.dell.com for å finne en liste over fingeravtrykkslesere som støttes.

Deaktivere pre-Windows-pålogging
Du kan også deaktivere pre-Windows-pålogging fra dette vinduet. For å gjøre det må du oppgi det gjeldende pre-Windows-passordet (systempassordet), bekrefte at passordet er riktig, og deretter klikke på **Deaktiver**-knappen. Vær oppmerksom på at eventuelle registrerte fingeravtrykk eller smartkort fremdeles vil være registrert når du deaktiverer pre-Windows-pålogging.

Registrer fingeravtrykk

Du kan registrere eller oppdatere fingeravtrykk som kan brukes ved godkjenning til systemet ved pre-Windows- eller Windows-pålogging. Hvis det er registrert fingeravtrykk, vises det en hånd i kategorien Fingeravtrykk som viser hvilke fingrer som er registrert. Hvis du klikker på koblingen **Registrer et annet**, startes veiviseren for registrering av fingeravtrykk, og du blir veiledet gjennom registreringsprosessen. Å registrere et fingeravtrykk betyr å lagre det for bruk ved pålogging. En gyldig fingeravtrykksleser må være riktig installert og konfigurert for å kunne registrere fingeravtrykk.

MERK: Enkelte fingeravtrykkslesere kan ikke brukes til pre-Windows-pålogging. Det vises en feilmelding hvis du prøver å registrere for pre-Windows-pålogging med en leser som ikke er kompatibel. Kontakt systemadministrator for å få vite om en bestemt enhet er kompatibel, eller gå til support.dell.com for å finne en liste over fingeravtrykkslesere som støttes.

Når du skal registrere fingeravtrykk, blir du bedt om å bekrefte identiteten ved å oppgi Windows-passordet ditt. Hvis policyen krever det, blir du også bedt om å oppgi pre-Windows-passordet (systempassordet). Pre-Windows-passordet kan brukes til å få tilgang til systemet hvis det er et problem med fingeravtrykksleseren.

MERKNADER:

- Det anbefales å registrere minst to fingeravtrykk i registreringsprosessen.
- Du må sørge for at fingeravtrykk er riktig registrert før godkjenning med fingeravtrykk aktiveres.
- Hvis du bytter ut en fingeravtrykksleser i et system, må du registrere fingeravtrykkene på nytt med den nye leseren. Å bytte frem og tilbake mellom to forskjellige fingeravtrykkslesere anbefales ikke.
- Hvis meldingen "Føleren mistet fokus" vises gjentatte ganger når du registrerer fingeravtrykk, kan det bety at datamaskinen ikke gjenkjenner fingeravtrykksleseren. Hvis det er en ekstern fingeravtrykksleser, kan dette problemet ofte løses ved å koble fra fingeravtrykksleseren og koble den til på nytt.

Slette registrerte fingeravtrykk
Du kan slette registrerte fingeravtrykk ved å klikke på koblingen **Slett fingeravtrykk** eller ved å klikke på (for å fjerne merket for) en registrert finger i veiviseren for registrering av fingeravtrykk.

Hvis du vil fjerne en bestemt bruker som det er registrert fingeravtrykk for pre-Windows-godkjenning for, kan administratoren fjerne merket for alle fingeravtrykk som er registrert for den aktuelle brukeren.

MERK: Hvis det oppstår feil under prosessen med registrering av fingeravtrykk, kan du se wave.com/support/Dell for å finne mer informasjon.

Registrere smartkort

Dell Data Protection | Access gir deg mulighet til å bruke tradisjonelle (med kontakt) smartkort eller smartkort uten kontakt ved pålogging til Windows-kontoer eller til pre-Windows-godkjenning. Klikk på koblingen **Registrer et annet smartkort** i kategorien Smartkort for å starte registreringsveiviseren for smartkort og bli veiledet gjennom registreringsprosessen. Å registrere smartkortet betyr å konfigurere pålogging ved bruk av kortet.

En gyldig smartkortgodkjenningsenhet må være riktig installert og konfigurert for å kunne utføre registrering.

MERK: Kontakt systemadministrator for å få vite om en bestemt enhet er kompatibel, eller gå til support.dell.com for å finne en liste over smartkort som støttes.

Registrering
Når du skal registrere et smartkort, blir du bedt om å bekrefte identiteten ved å oppgi Windows-passordet ditt. Hvis policyen krever det, blir du også bedt om å oppgi pre-Windows-passordet (systempassordet). Pre-Windows-passordet kan brukes til å få tilgang til systemet hvis det er et problem med smartkortleseren.

Hvis det er angitt en PIN-kode for smartkortet, blir du bedt om å oppgi dette under registreringen. Hvis policyen krever en PIN-kode og det ikke er angitt en, blir du bedt om å lage en.

MERKNADER:

- Når en bruker er registrert for bruk av smartkort i ved pre-Windows-pålogging, kan ikke brukeren fjernes.
- Standardbrukere kan endre bruker-PIN-koden på et smartkort, og administratoren kan endre både administrator-PIN-koden og bruker-PIN-koden.
- Administratoren kan også tilbakestille et smartkort. Når kortet er tilbakestilt, kan det ikke brukes til godkjenning ved Windows-pålogging eller pre-Windows-pålogging før det registreres.

MERK:Når det gjelder godkjenning med TPM-sertifikater, kan administratorer registrere TPM-sertifikater med Microsoft Windows-prosessen for registrering av smartkort. Administratorer må velge Wave TCG Activated CSP som kryptografitjeneste i stedet for en smartkort-CSP for kompatibilitet med dette programmet. I tillegg må sikker Dell-pålogging aktiveres med den riktige godkjenningstypepolicyen for klienten.

MERK: Hvis det vises en feilmelding om at Smart Card-tjenesten ikke kjører, kan du starte denne tjenesten eller starte den på nytt ved å gjøre følgende:

- Naviger til vinduet Administrative verktøy fra Kontrollpanel, velg Tjenester, og høyreklikk på Smart Card og velg Start eller Start på nytt.
- Hvis du vil ha mer informasjon om en bestemt feilmelding, kan du gå til wave.com/support/Dell.

Oversikt over Self-Encrypting Drive

Dell Data Protection | Access behandler de maskinbaserte sikkerhetsfunksjonene på selvkrypterende stasjoner som har datakryptering innebygget i stasjonsmaskinvaren. Denne funksjonaliteten sikrer at bare autoriserte brukere får tilgang til krypterte data (når stasjonslåsing er aktivert).

Vinduet Self-Encrypting Drive åpnes ved å klikke på den nederste kategorien **Self-Encrypting Drive**. Denne kategorien vises bare når én eller flere selvkrypterende stasjoner (SEDer) finnes i systemet.

Klikk på koblingen **Oppsett** for å starte veiviseren for Self-Encrypting Drive-oppsett. I denne veiviseren oppretter du et stasjonsadministratorpassord, sikkerhetskopierer dette passordet og tar i bruk innstillingene for stasjonskryptering. Bare systemadministratorer har tilgang til veiviseren for Self-Encrypting Drive-oppsett.

Viktig! Når en stasjon blir konfigurert, "aktiveres" stasjonslåsing og databeskyttelse. Når en stasjon er låst, fungerer den på følgende måte:

- Stasjonen går til *låst* modus når stasjonen slås av.
- Stasjonen vil ikke starte opp før du oppgir riktig brukernavn og passord (eller fingeravtrykk) i skjermbildet Pre-Windows-pålogging. Før stasjonslåsing aktiveres har alle brukere av datamaskinen tilgang til data på stasjonen.
- Stasjonen er også sikret hvis den kobles til en annen datamaskin som en sekundær stasjon, og det kreves godkjenning for å få tilgang til stasjonsdataene.

Når stasjonen har blitt konfigurert, viser vinduet Self-Encrypting Drive stasjonen(e) og en kobling brukerne kan bruke til å endre stasjonspassordet sitt. Hvis du er stasjonsadministrator, kan du også legge til eller slette stasjonsbrukere fra dette vinduet. Hvis det er konfigurert en ekstern stasjon, vil den bli vist i dette vinduet og kan låses opp.

MERK: For å kunne låse en sekundær, ekstern stasjon må stasjonen slås av uavhengig fra datamaskinen.

Stasjonsadministratoren kan behandle stasjonsinnstillingene i **Avansert>Enheter**. Hvis du vil ha mer informasjon, kan du se Enhetsbehandling – Self-Encrypting Drive-enheter.

Stasjonsoppsett

Veiviseren for Self-Encrypting Drive-oppsett veileder deg gjennom konfigurasjon av stasjonen(e). Det er viktig å være klar over konseptene nedenfor når du går gjennom denne prosessen.

Stasjonsadministrator
Den første brukeren med administratorrettigheter som konfigurerer stasjonstilgang (og angir stasjonsadministratorpassordet), bli stasjonsadministrator. Dette blir den eneste brukeren med rettigheter til å endre stasjonstilgang. For å sikre at den første brukeren er ment å bli konfigurert som stasjonsadministrator, må du merke av for "Jeg forstår" for å fortsette med dette trinnet.

Stasjonsadministratoradministratorpassord
Veiviseren ber deg opprette et stasjonsadministratorpassord og bekrefte passordet ved å skrive det inn på nytt. Du må skrive inn Windows-passordet for å angi identiteten din før du kan opprette stasjonsadministratorpassordet. Den aktuelle Windows-brukeren må ha administratorrettigheter for å opprette dette passordet.

Sikkerhetskopier stasjonslegitimasjon
Skriv inn en plassering, eller klikk på **Bla gjennom**-knappen for å velge en plassering, for å lagre en sikkerhetskopi av stasjonsadministratorlegitimasjonen.

VIKTIG**!**

- Det anbefales sterkt å sikkerhetskopiere denne legitimasjonen og at du sikkerhetskopierer den til en annen stasjon en den primære harddisken (for eksempel et flyttbar medium). Hvis du ikke gjør det, får du ikke tilgang til sikkerhetskopien hvis du mister tilgang til stasjonen.
- Når stasjonsoppsettet er fullført, må eventuelle brukere oppgi sitt riktige brukernavn og passord (eller fingeravtrykk) før Windows lastes inn, for å få tilgang til systemet nestet gang systemet slås på.

Legg til stasjonsbruker
Stasjonsadministratoren kan legge til andre stasjonsbrukere som er gyldige Windows-brukere. Når administratoren legger til brukere for stasjonen, kan det kreves at den brukeren tilbakestiller passordet ved første pålogging. Brukeren vil bli bedt å tilbakestille passordet i skjermbildet for pre-Windows-pålogging før stasjonen kan låses opp.

Avanserte innstillinger

- *Single Sign On* – Som standard brukes Self-Encrypting Drive-passordet som du oppgir ved pre-Windows-pålogging, automatisk brukes til å logge deg på Windows også (dette kalles Single Sign On). Hvis du vil deaktivere denne funksjonen, merker du av for "Jeg vil logge på på nytt når Windows starter" når du konfigurerer stasjonsinnstillingene.
- *Fingeravtrykkpålogging* – På plattformer som støttes, kan du angi at du utføre godkjenning for den selvkrypterende stasjonen ved å bruke et fingeravtrykk i stedet for et passord.
- *Støtte for ventemodus/hvilemodus (S3)* (hvis dette støttes på plattformen) – Hvis dette aktiveres, kan den selvkrypterende stasjonen sikkert plasseres i ventemodus/hvilemodus (også kalt S3-modus), og det vil bli krevd pre-Windows-godkjenning for å fortsette etter ventemodus/hvilemodus.

MERKNADER:

- Når S3-støtte er aktivert, gjelder eventuelle BIOS-passordbegrensninger som finnes, for stasjonspassordene. Kontakt produsenten av systemmaskinvaren for å få mer informasjon om eventuelle spesifikke BIOS-passordbegrensninger som måtte finnes for systemet.
- Enkelte selvkrypterende stasjoner støtter ikke S3-modus. Når stasjonen konfigureres, vil du bli varslet om stasjonen støtter ventemodus/hvilemodus eller ikke. For stasjoner som ikke støtter denne modusen, vil Windows S3-forespørsler automatisk bli konvertert til dvaleforespørsler, hvis dvalemodus er aktivert (det anbefales sterkt at du aktiverer dvalemodus på stasjonen).
- Første gang du logger deg på etter at alternativet Single Sign On (SSO) er angitt, vil prosessen ta en pause når det bes om Windows-pålogging. Du blir bedt om å oppgi din form for Windows-godkjenning, og denne vil bli lagret sikkert for fremtidige forsøk på Windows-pålogging. Neste gang systemet startes opp, logger SSO deg automatisk på Windows. Den samme prosessen kreves også når en brukers Windows-godkjenning (passord, fingeravtrykk, smartkort-PIN-kode) endres. Hvis datamaskinen er på et domene og dette domenet har en policy som krever at det skal trykkes på ctrl+alt+del for Windows-pålogging, tas det hensyn til denne policyen.

ADVARSEL:Hvis du avinstallerer programmet **Dell Data Protection | Access**, må du først deaktivere databeskyttelse for den selvkrypterende stasjonen og låse opp stasjonen.

Funksjoner for SED-brukere

Administratorer av selvkrypterende stasjoner kan utføre all behandling av stasjonssikkerhet og -brukere. Stasjonsbrukere som ikke er stasjonsadministrator, kan bare utføre disse oppgavene:

- endre sitt eget passord
- låse opp en stasjon

Disse oppgavene kan utføres fra kategorien **Self-Encrypting Drive** i **Dell Data Protection | Access**.

Endre passord
Dette gir registrerte brukere mulighet til å opprette et nytt passord for stasjonsgodkjenning. Du må oppgi det gjeldende Self-Encrypting Drive-passordet før stasjonspassordet angis til den nye verdien.

MERKNADER:

- Programmet fremtvinger bruk av policyene for Windows-passordets lengde og kompleksitet hvis disse er aktivert. Hvis policyene for Windows-passord ikke er aktivert, er maksimal lengde for et Self-Encrypting Drive-passord på 32 tegn. Vær oppmerksom på at maksimal lengde er 127 tegn hvis S3 (ventemodus/hvilemodus) ikke er aktivert.
- Self-Encrypting Drive-passordet er forskjellig fra Windows-passordet. Når Windows-passord endres eller tilbakestilles, har det ingen betydning for stasjonspassordet med mindre synkronisering med Windows-passord er aktivert. Se Enheter: Self-Encrypting Drive-enheter hvis du vil ha mer informasjon.
- På enkelte ikke-engelske tastaturer er det et sett med begrensete tegn som ikke kan brukes i passord for selvkrypterende stasjoner. Hvis Windows-passordet inneholder noen av de begrensede tegnene og synkronisering med Windows-passord er aktivert, vil synkroniseringen mislykkes og du vil få en feilmelding.

Stasjonsopplåsing
Stasjonsopplåsing gir en registrert stasjonsbruker mulighet til å låse opp en låst stasjon. Hvis stasjonslåsing er aktivert, settes stasjonen i låst tilstand når strømmen til datamaskinen slås av. Når systemet slås på igjen, må du godkjennes for stasjonen ved å oppgi passordet ditt i skjermbildet for pre-Windows-godkjenning.

MERKNADER:

- Manglende evne til å gå til strømsparingsmodus (det vil si ventemodus/hvilemodus eller dvalemodus) kan oppstå hvis flere brukerkonti for selvkrypterende stasjoner er aktive samtidig på datamaskinen.
- I skjermbildet for pre-Windows-godkjenning erstatter bruker 1, bruker 2 og så videre stasjonsbrukernavnene i versjoner av TDM som er lokalisert for følgende språk: kinesisk, japansk, koreansk og russisk.

Avanserte alternativer

Ved hjelp av de avanserte alternativene i **Dell Data Protection | Access** kan en bruker med administratorrettigheter administrere følgende i programmet:

Vedlikehold
Passord
Enheter

MERK: Bare brukere med administratorrettigheter kan gjøre endringer i avanserte alternativer. Standardbrukere kan vise disse innstillingene, men ikke gjøre endringer.

Oversikt over vedlikehold

Vedlikehold-vinduet kan brukes av administratorer til å konfigurere innstillinger for Windows-pålogging, tilbakestille et system for å klargjøre det til nye oppgaver eller arkivere eller gjenopprette brukerlegitimasjoner som er lagret i systemets sikkerhetsmaskinvare. Se følgende emner for å finne mer informasjon:

Tilgangsinnstillinger
Tilbakestill system
Legitimasjonsarkivering og -gjenoppretting

Tilgangsinnstillinger

I vinduet Tilgangsinnstillinger kan administratorer angi innstillinger for Windows-pålogging for alle brukere av systemet.

Aktiver sikker Dell-pålogging
Ved hjelp av alternativet som erstatter standardskjermbildet som åpnes med ctrl-alt-delete i Windows, kan du bruke forskjellige godkjenningsfaktorer i stedet for (eller i tillegg til) Windows-passordet for tilgang til Windows. Du kan velge å legge til et fingeravtrykk som en ekstra godkjenningsfaktor for å styrke sikkerheten i Windows-påloggingsprosessen. Andre godkjenningsfaktorer kan også legges til for pålogging til Windows, inkludert et smartkort eller TPM-sertifikat.

MERKNADER:

- Aktivering av sikker Dell-pålogging påvirker alle brukere i systemet.
- Det anbefales å aktivere dette alternativet ETTER at brukere har registrert sine fingeravtrykk eller smartkort.
- Første gang du logger deg på etter at dette alternativet er angitt, vil du bli bedt om godkjenning for Windows i henhold til standardpolicyen, og deretter må du bruke din(e) nye godkjenningsfaktor(er) ved neste oppstart.

Deaktiver sikker Dell-pålogging
Dette alternativet deaktiverer alle **Dell Data Protection | Access**-funksjoner for pålogging til Windows. Når alternativet velges, går systemet tilbake til standard Windows-påloggingspolicy.

MERKNADER:

- Hvis det oppstår feil i forbindelse med sikker Windows-pålogging når du prøver å logge deg på, kan du deaktivere og deretter aktivere på nytt alternativet for sikker Dell-pålogging.
- Hvis du vil ha mer informasjon om en bestemt feilmelding, kan du gå til wave.com/support/Dell.

Tilbakestill system

Funksjonen Tilbakestill system brukes til å slette alle brukerdata fra all sikkerhetsmaskinvare på plattformen. Den kan for eksempel brukes når en datamaskin skal klargjøres for nye oppgaver. Dette alternativet sletter alle passord i systemet bortsett fra passordene for Windows-brukere, og i tillegg slettes alle data i maskinvareenhetene (for eksempel ControlVault, TPM og fingeravtrykkslesere). Funksjonen deaktiverer også databeskyttelse for selvkrypterende stasjoner slik at stasjonsdataene blir tilgjengelige.

Du må bekrefte at du forstår at du tilbakestiller systemet, og deretter klikke på **Neste**. For å tilbakestille systemet må du oppgi passordet for hver enkelt sikkerhetsenhet hvis det er angitt passord for dem:

- TPM-eier
- ControlVault-administrator
- BIOS-administrator
- BIOS-system (pre-Windows)
- Harddisk (BIOS)
- Self-Encrypting Drive-administrator

MERK: For selvkrypterende stasjoner kreves bare passordet for stasjonsadministrator, ikke passordene for alle brukerne av stasjonen.

Viktig! Den eneste måten å gjenopprette data som slettes ved tilbakestilling av systemet, er å gjenopprette fra et tidligere lagret arkiv. Hvis du ikke har et arkiv, kan disse dataene ikke gjenopprettes. På en selvkrypterende stasjon slettes bare konfigurasjonsdataene. Ingen personlige data slettes på stasjonen.

Legitimasjonsarkivering og -gjenoppretting

Funksjonaliteten for legitimasjonsarkivering og -gjenoppretting brukes til å sikkerhetskopiere eller gjenopprette alle brukerlegitimasjoner (informasjon om pålogging og kryptering) som er lagret i ControlVault og Trusted Platform Module (TPM). Å ha en sikkerhetskopi av dataene er viktig når du vil oppgradere en datamaskin eller gjenopprette data ved maskinvarefeil. I slike tilfeller gjenoppretter du bare alle legitimasjonene til den nye datamaskinen fra en lagret arkivfil.

Du kan velge å arkivere eller gjenopprette legitimasjoner for en enkeltbruker eller alle brukerne i systemet.

Brukerlegitimasjonen består av data som brukes ved pre-Windows-pålogging, som registrerte fingeravtrykk og smartkortdata og nøkler lagret i TPM. TPM oppretter nøkler etter forespørsler fra sikre programmer. Det opprettes for eksempel nøkler i TPM ved generering av et digitalt sertifikat.

MERK: For å finne ut om TPM-nøklene kan arkiveres av **Dell Data Protection | Access**, kan du slå opp i dokumentasjonen for det sikre programmet. Generelt støttes generering av nøkler i programmer som bruker Wave TCG Activated CSP til å generere nøkler.

Arkivere legitimasjoner
Følgende må gjøres for å arkivere legitimasjoner:

- Angi om du vil arkivere legitimasjonen for deg selv eller for alle brukere i systemet.
- Sørg for godkjenning til den sikre maskinvaren ved å oppgi systempassordet (pre-Windows-passordet), ControlVault-administratorpassordet og TPM-eierpassordet.
- Opprett et passord for legitimasjonssikkerhetskopien.
- Angi en arkivplassering ved hjelp av **Bla gjennom**-knappen. Arkivplasseringen må være et flyttbart medium, for eksempel en USB-flashstasjon eller nettverksstasjon, for å få beskyttelse mot harddiskfeil.

Viktige merknader:
- Noter deg arkivplasseringen. Brukeren trenger denne informasjonen for å gjenopprette legitimasjonsinformasjonen.
- Noter deg passordet for legitimasjonssikkerhetskopien slik at det blir mulig å gjenopprette disse dataene. Dette er viktig fordi passordet ikke kan gjenopprettes.
- Hvis du ikke kjenner TPM-eierpassordet, må du kontakte systemadministrator eller slå opp i datamaskinens instruksjoner for konfigurering av TPM.

Gjenopprette legitimasjoner
Følgende må gjøres for å gjenopprette legitimasjoner:

- Angi om du vil gjenopprette legitimasjonen for deg selv eller for alle brukere i systemet.
- Bla frem til arkivplasseringen, og velg arkivfilen.
- Oppgi passordet som ble opprettet for legitimasjonssikkerhetskopien da du konfigurerte arkivet.
- Sørg for godkjenning til den sikre maskinvaren ved å oppgi systempassordet (pre-Windows-passordet), ControlVault-administratorpassordet og TPM-eierpassordet.

MERKNADER:
- Hvis det vises en feilmelding om at gjenoppretting av legitimasjonene mislykkes og du har prøvde flere ganger å utføre en gjenoppretting, prøver du å gjenopprette for en annen arkivfil. Hvis dette ikke lykkes, lager du et nytt legitimasjonsarkiv og prøver å gjenopprette fra det nye arkivet.

- Hvis det vises en feilmelding om at TPM-nøkler ikke kunne gjenopprettes, tømmer du TPM i BIOS. For å tømme TPM starter du datamaskinen på nytt og trykker på **F2**-tasten når du starter sikkerhetskopieringen, for å få tilgang til BIOS-innstillingene, og deretter navigerer du til Security>TPM Security. Gjenopprett eierskap til TPM, og prøv på nytt å gjenopprette legitimasjonen(e).
- Hvis du vil ha mer informasjon om en bestemt feilmelding, kan du gå til wave.com/support/Dell.

Passordbehandling

Fra vinduet Passordbehandling kan en administrator opprette eller endre alle sikkerhetspassordene i systemet:

- Systempassord (også kalt pre-Windows-passord)*
- Administratorpassord*
- Harddiskpassord*
- ControlVault-passord
- TPM-eierpassord
- TPM- hovedpassord
- TPM-passordhvelvpassord
- Self-Encrypting Drive-passord

MERKNADER:

- Bare passord som brukes i den gjeldende plattformkonfigurasjonen, vil bli vist, så dette vinduet endres avhengig av systemets konfigurasjon og status.
- Passordene ovenfor som er merket med med *, er BIOS-passord og kan også endres via system-BIOS.
- Passordene på BIOS-nivå kan ikke opprettes eller endres hvis BIOS-administratoren har nektet endring av passord.
- Hvis du klikker på koblingen **konfigurer** for en selvkrypterende stasjon, startes veiviseren for Self-Encrypting Drive-oppsett. Hvis du klikker på koblingen **behandle**, kan du endre ett eller flere Self-Encrypting Drive-passord.
- Hvis du klikker på koblingen **behandle** for TPM-passordhvelvet, vises det et vindu der du kan vise eller endre passordene som beskytter TPM-nøklene dine. Når det opprettes en TPM-nøkkel som krever at det opprettes et passord, genereres det et tilfeldig passord, og dette plasseres i hvelvet. Du kan ikke behandle TPM-passordhvelvet før du har opprettet et TPM-hovedpassord.

Kompleksitetsregler for Windows-passord

Dell Data Protection | Access sikrer at følgende passord samsvarer med kompleksitetsreglene for Windows-passord på maskinen:

- TPM-eierpassord

Følg denne fremgangsmåten for å finne kompleksitetspolicyen for Windows-passord på maskinen:

1. Gå til Kontrollpanel.
2. Dobbeltklikk på Administrative verktøy.
3. Dobbeltklikk på Lokal sikkerhetspolicy.
4. Utvid Kontopolicyer, og velg Passordpolicy.

Oversikt over enheter

Enheter-vinduet brukes av administratorer til å administrere alle sikkerhetsenhetene som er installert i systemet. For hver enhet kan du vise statusen og detaljert tilleggsinformasjon, for eksempel programvareversjonen. Klikk på **vis** for å vise informasjonen for hver enhet, eller klikk på **skjul** for å skjule en seksjon. Avhengig av hva plattformen inneholder kan følgende enheter administreres:

Trusted Platform Module (TPM)
ControlVault®
Self-Encrypting Drive-enhet(er)
Informasjon om godkjenningsenheter

Trusted Platform Module (TPM)

TPM-sikkerhetsbrikken må aktiveres og eierskap for TPM må opprettes for å kunne bruke de avanserte sikkerhetsfunksjonene som er tilgjengelige for **Dell Data Protection | Access** og TPM.

Vinduet Trusted Platform Module i **Enhetsbehandling** vises bare når det oppdages en TPM i systemet.

TPM-behandling

Med disse funksjonene kan systemadministrator administrere TPM.

Status
Viser statusen *aktiv* eller *inaktiv* for TPM. Statusen "Aktiv" betyr at TPM er aktivert i BIOS og er klar til å konfigureres (det vil si at eierskap kan tas). TPM kan ikke behandles, og du får ikke tilgang til dens sikkerhetsfunksjoner, hvis TPM ikke er aktiv (aktivert).

Hvis TPM oppdages i systemet, men ikke er aktiv (aktivert), kan du aktivere ved å klikke på koblingen **aktiver** i dette vinduet uten å gå til system-BIOS. Når TPM aktiveres med denne funksjonen, må datamaskinen startes på nytt. Når den startes på nytt, kan du i enkelte tilfeller bli bedt om å godta endringene.

MERK: Muligheten til å aktivere TPM fra dette programmet støttes ikke på alle plattformer. Hvis det ikke støttes, må du aktivere i system-BIOS. Det gjør du ved å starte datamaskinen og trykke på **F2**-tasten før Windows lastes inn, for å få tilgang til BIOS-innstillingene, og deretter navigerer du til Security>TPM Security og aktiverer TPM.

Du kan også *deaktivere* TPM herfra ved å klikke på koblingen **deaktiver**. Deaktivering av TPM vil gjøre den utilgjengelig for de avanserte sikkerhetsfunksjonene. Deaktivering sletter imidlertid ikke noen av TPM-innstillingene, og eventuell informasjon eller nøkler som er lagret i TPM. slettes eller endres heller ikke.

Eiet
Viser statusen til eierskap (det vil si "eiet") , og lar deg opprette eller endre TPM-eieren. TPM-eierskap må opprettes for at sikkerhetsfunksjonen skal bli tilgjengelig. Før eierskapet kan etableres må TPM aktiveres.

Prosessen med etablering av eierskap består av at brukeren (med administratorrettigheter) oppretter et TPM-eierpassord. Når dette passordet er definert, etableres eierskapet og TPM er klar for bruk.

MERK: TPM-eierpassordet må samsvare med kompleksitetsreglene for Windows-passord for systemet.

Viktig! Det er viktig at du ikke mister eller glemmer TPM-eierpassordet da dette kreves for å få tilgang til avanserte sikkerhetsfunksjoner for TPM i **Dell Data Protection | Access**.

Låst
Viser statusen *låst* eller *ulåst* for TPM. "Låsing" er en sikkerhetsfunksjon i TPM. TPM vil gå til låst tilstand etter et angitt antall forsøk på å oppgi feil TPM-eierpassord. TPM-eieren kan låse opp TPM herfra. Det kreves at TPM-eierpassordet oppgis.

MERKNADER:

- Hvis det vises en feilmelding om at eierskapet til TPM ikke kunne etableres, tømmer du TPM i system-BIOS og prøver å etablere eierskap på nytt. For å tømme TPM starter du

datamaskinen på nytt og trykker på **F2**-tasten når du starter sikkerhetskopieringen, for å få tilgang til BIOS-innstillingene, og deretter navigerer du til Security>TPM Security.

- Hvis det vises en feilmelding om at TPM-eierpassordet ikke kunne endres, arkiverer du TPM-dataene (legitimasjonsarkiv), tømmer TPM i BIOS, etablerer nytt TPM-eierskap og gjenoppretter TPM-data (gjenoppretter legitimasjon).
- Hvis du vil ha mer informasjon om en bestemt feilmelding, kan du gå til wave.com/support/Dell.

Dell ControlVault®

Dell ControlVault® (CV) er et sikkert maskinvarelager for brukerlegitimasjoner som brukes ved pre-Windows-pålogging (for eksempel fingeravtrykk eller registrerte fingeravtrykksdata). ControlVault-vinduet i **Enhetsbehandling** vises bare når det oppdages et ControlVault i systemet.

ControlVault-behandling

Med disse funksjonene kan systemadministrator behandle systemets ControlVault.

Status
Viser statusen *aktiv* eller *inaktiv* for ControlVault. Statusen Inaktiv betyr at ControlVault ikke er tilgjengelig for lagring i systemet. Slå opp i dokumentasjonen for Dell-systemet for å finne ut om systemet inneholder et ControlVault.

Passord
Viser om det er konfigurert et ControlVault-administratorpassord, og lar deg konfigurere et passord eller endre passordet (hvis det allerede er konfigurert et). Det er bare systemadministratorer som kan konfigurere eller endre dette passordet. Et ControlVault-administratorpassord må angis for å kunne gjøre følgende:

- Utføre en legitimasjonsarkivering eller -gjenoppretting.
- Slette brukerdata (for alle brukere).

Merk: Hvis en bruker prøver å arkivere eller gjenopprette når ControlVault-administratorpassordet ikke er angitt, blir hun/han bedt om å opprette et (hvis brukeren er administrator).

Registrerte brukere
Viser om det for øyeblikket er registrert legitimasjoner (for eksempel passord, fingeravtrykk eller smartkortdata) for noen brukere, som er lagret i ControlVault.

Slett brukerdata
Det kan hende dataene i ControlVault på et eller annet tidspunkt må slettes, for eksempel hvis brukere har problemer med å bruke eller registrere Pre-Windows-legitimasjoner for godkjenning. Alle data som er lagret i ControlVault, kan slettes fra dette vinduet, enten for en enkeltbruker eller alle brukerne.

ControlVault-administratorpassordet må oppgis for å slette alle brukerdata på plattformen. Du vil også bli bedt om å oppgi systempassordet (pre-Windows-passordet) hvis det er registrert pre-Windows-legitimasjoner. Når du sletter alle brukerdata, tilbakestilles ControlVault-administratorpassordet og systempassordet. Merk deg at dette er eneste måte å slette ControlVault-administratorpassordet på.

MERK: Når du sletter alle brukerdata, blir du bedt om å starte datamaskinen på nytt. Det er viktig å starte på nytt for å få systemet til å fungere riktig.

ControlVault-administratorpassordet trenger ikke å angis for å slette legitimasjonen for en enkeltbruker. Når du klikker på **fjern brukerdata**, blir du bedt om å velge hvem ControlVault-legitimasjonen skal slettes for. Når du velger en bruker, blir du bedt om å oppgi systempassordet (bare hvis pre-Windows-legitimasjon er registrert).

MERKNADER:

- Hvis det vises en feilmelding om at ControlVault-administratorpassordet ikke kan opprettes, må du arkivere legitimasjonene, fjerne alle brukerdata fra ControlVault, starte datamaskinen på nytt og prøve å opprette passordet på nytt.
- Hvis det vises en feilmelding om at legitimasjonene ikke kunne fjernes fra ControlVault for en enkeltbruker, må du arkivere legitimasjonene, prøve å fjerne alle brukerdata og deretter på nytt prøve å fjerne data for denne brukeren.
- Hvis det vises en feilmelding om at legitimasjonene ikke kunne fjernes fra ControlVault for alle brukere, bør du vurdere om du skal utføre en tilbakestilling av systemet. **Viktig!** Se gjennom emnet om tilbakestilling av systemet før du utfører en tilbakestilling, da dette vil slette ALLE brukersikkerhetsdata.
- Hvis det vises en feilmelding om at ControlVault- og TPM-data ikke kunne sikkerhetskopieres, deaktiverer du TPM i system-BIOS. Det gjør du ved å starte datamaskinen på nytt og trykke på **F2**-tasten når du starter sikkerhetskopieringen, for å få tilgang til BIOS-innstillingene, og deretter navigerer du til Security>TPM Security. Aktiver deretter TPM igjen, og prøv på nytt å arkivere ControlVault-dataene.
- Hvis du vil ha mer informasjon om en bestemt feilmelding, kan du gå til wave.com/support/Dell.

Self-Encrypting Drives: Avansert

Dell Data Protection | Access behandler de maskinbaserte sikkerhetsfunksjonene på selvkrypterende stasjoner som har datakryptering innebygget i stasjonsmaskinvaren. Denne behandlingen sikrer at bare autoriserte brukere får tilgang til krypterte data når stasjonslåsing er aktivert.

Vinduet Self-Encrypting Drive i **Enhetsbehandling** vises bare hvis én eller flere selvkrypterende stasjoner (SED) finnes i systemet.

Viktig! Når en stasjon blir konfigurert, "aktiveres" stasjonslåsing og beskyttelse av data på den selvkrypterende stasjonen.

Stasjonsbehandling
Med disse funksjonene kan stasjonsadministratoren behandle innstillinger for stasjonssikkerhet. Endringer i innstillingene for stasjonssikkerhet trer i kraft etter at stasjonen har blitt slått av.

Databeskyttelse
Viser statusen *aktivert* eller *deaktivert* for databeskyttelse på den selvkrypterende stasjonen. Statusen "aktivert" betyr at stasjonssikkerhet er konfigurert, men før stasjons*låsing* blir aktivert trenger ikke brukerne å godkjennes for stasjonen med pre-Windows-pålogging for å få tilgang.

Du kan deaktivere databeskyttelse på den selvkrypterende stasjonen herfra. Når databeskyttelsen er deaktivert, er alle avanserte sikkerhetsfunksjoner på den selvkrypterende stasjonen slått av, og stasjonen fungerer som en standardstasjon. Deaktivering av databeskyttelsen sletter også alle sikkerhetsinnstillinger inkludert legitimasjonen til stasjonsadministratoren og stasjonsbrukerne. Funksjonen vil imidlertid ikke endre eller slette brukerdata på stasjonen.

Låsing
Viser statusen *aktivert* eller *deaktivert* for de(n) selvkrypterende stasjonen(e). Se emnet Self-Encrypting Drive for å finne informasjon om hvordan en låst stasjon fungerer.

Det kan bli nødvendig å midlertidig deaktivere stasjonslåsing, og det kan du gjøre herfra. Dette anbefales ikke fordi det ikke kreves legitimasjon for å få tilgang til stasjonen når stasjonslåsing er deaktivert, så alle plattformbrukere kan få tilgang til dataene. Deaktivering av stasjonslåsingsletter ikke noen av sikkerhetsinnstillingene, inkludert legitimasjonene til stasjonsadministratoren og stasjonsbrukerne, eller andre brukerdata på stasjonen.

ADVARSEL: Hvis du avinstallerer programmet **Dell Data Protection | Access**, må du først deaktivere databeskyttelse for den selvkrypterende stasjonen og låse opp stasjonen.

Stasjonsadministrator

Viser gjeldende stasjonsadministrator. Herfra kan stasjonsadministratoren endre hvilken bruker som skal være stasjonsadministrator. Den nye administratoren må være en gyldig Windows-bruker med administratorrettigheter i systemet. Systemet kan ha bare én stasjonsadministrator.

Stasjonsbrukere

Viser de registrerte stasjonsbrukerne og antall brukere som for øyeblikket er registrert. Maksimalt antall brukere som støttes, baseres på typen selvkrypterende stasjon (for tiden 4 brukere for Seagate-stasjoner og 24 for Samsung-stasjoner).

Synkronisering med Windows-passord
Funksjonen for synkronisering med Windows-passord (WPS) setter automatisk brukernes Self-Encrypting Drive-passord til å være det samme som Windows-passordet. Denne funksjonen blir ikke gjennomført for stasjonsadministratoren, den gjelder bare for stasjonsbrukere. WPS-funksjonen kan brukes i bedriftsmiljøer der passordene må endres med bestemte tidsintervall (for eksempel hver 90. dag). Når dette alternativet er aktivert, vil alle brukeres Self-Encrypting Drive-passord automatisk oppdateres når disse Windows-passordene endres.

MERK: Når synkronisering med Windows-passord (WPS) er aktivert, kan ikke en brukers Self-Encrypting Drive-passord endres. Brukerens Windows-passord må endres for å automatisk oppdatere stasjonspassordet.

Husk siste brukernavn
Når dette alternativet er aktivert, vises som standard det sist brukte brukernavnet i **Brukernavn**-feltet i skjermbildet for pre-Windows-godkjenning.

Velge brukernavn
Når dette alternativet er aktivert, kan brukerne vise alle brukernavnene i **Brukernavn**-feltet i skjermbildet for pre-Windows-godkjenning.

Kryptografisk sletting
Dette alternativet kan brukes til å "slette" alle data på den selvkrypterende stasjonen. Dette sletter egentlig ikke dataene, men sletter nøklene som brukes til å kryptere dataene, slik at dataene ikke kan brukes. Det finnes ingen måte å gjenopprette stasjonsdata på etter en kryptografisk sletting. Beskyttelse av data på den selvkrypterende stasjonen deaktiveres også, og stasjonen er klar til å brukes til andre formål.

MERKNADER:
- Hvis det oppstår feil relatert til funksjonene for behandling av den selvkrypterende stasjonen, slår du datamaskinen helt av (ikke en omstart), og deretter starter du på nytt.
- Hvis du vil ha mer informasjon om en bestemt feilmelding, kan du gå til wave.com/support/Dell.

Informasjon om godkjenningsenheter

Vinduet Informasjon om godkjenningsenheter i **Enhetsbehandling** viser informasjon om og status for alle tilkoblede godkjenningsenheter (det vil si fingeravtrykksleser eller smartkortleser for vanlige kort eller kort uten kontakt) i systemet.

Teknisk støtte

Teknisk støtte for **Dell Data Protection | Access**-programvaren finnes på http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP

Wave Systems TCG Activated (Trusted Computing Group) CSP (Cryptographic Service Provider) er inkludert i programmet **Dell Data Protection | Access** og er tilgjengelig for bruk når det kreves en CSP – enten direkte oppkalt fra et program eller som valg fra en liste over installerte CSPer. Velg Wave TCG Activated CSP når det er mulig, for å sikre at TPM genererer nøkler, og at nøklene og passordene administrerers av **Dell Data Protection | Access**.

Ved hjelp av Wave Systems TCG Activated CSP kan programmer bruke funksjoner som er tilgjengelige på TCG-kompatible plattformer, direkte via MSCAPI. Den er en TCG-forbedret MSCAPI CSP-modul som gir funksjonalitet for asymmetriske nøkler på TPM og leverer forbedret sikkerhet med TPM uavhengig av leverandørspesifikke krav angående TSS-leverandøren (Trusted Software Stack).

MERK: Hvis TPM-nøklene som genereres av Wave TCG Activated CSP krever et passord og brukeren har opprettet et TPM-hovedpassord, genereres de individuelle nøkkelpassordene tilfeldig og lagres i TPM-passordhvelvet.