Dell Data Protection | Adgang (Access) - startside

Startsiden for **Dell Data Protection | Adgang (Access)** er udgangspunktet for at få adgang til funktionerne i programmet. Fra dette vindue kan du få adgang til følgende:

System Access Wizard
Indstillinger for adgang (Access Options)
Self-Encrypting Drive
Avancerede indstillinger (Advanced Options)

I nederste højre hjørne af vinduet vises linket **avanceret** (advanced), som du kan klikke på for at få vist avancerede indstillinger.

Fra de avancerede indstillinger kan du klikke på linket **startside** (home) i nederste højre hjørne af vinduet for at komme tilbage til startsiden.

System Access Wizard

System Access Wizard starter automatisk, første gang programmet **Dell Data Protection | Adgang (Access)** startes. Guiden fører dig gennem opsætning af alle aspekter af sikkerhed på systemet, herunder hvordan (f.eks. adgangskode eller fingeraftryk og adgangskode) og hvornår (ved Windows, Pre-Windows eller begge), du vil logge på systemet. Derudover kan du konfigurere SED, hvis der findes et, i denne guide.

Administratorfunktioner

Brugere, der er oprettet med Windows-administratorrettigheder på systemet, kan udføre følgende funktioner i **Dell Data Access | Beskyttelse (Protection)**, som standardbrugere ikke kan udføre:

- Angivelse/ændring af system (Pre-Windows) adgangskode
- Angivelse/ændring af adgangskode til harddisk
- Angivelse/ændring af administratoradgangskode
- Angivelse/ændring af adgangskode for TPM-ejer
- Angivelse/ændring af administratoradgangskode for ControlVault
- Nulstilling af system
- Arkivering og gendannelse af legitimationsoplysninger
- Angivelse/ændring af administrator-PIN-kode til smartcard
- Sletning/nulstilling af smartcard
- Aktivering/deaktivering af Dell sikker logon til Windows (Dell Secure Login)
- Angivelse af Windows-logonpolitik
- Administration af selvkrypterende drev, herunder:
    - Aktivering/deaktivering af selvkrypterende drevlås
    - Aktivering/deaktivering af Windows Password Synchronization (WPS)
    - Aktivering/deaktivering af Single Sign On (SSO)
    - Udførelse af kryptografisk sletning

Fjernadministration

Din virksomhed kan oprette et miljø, hvor sikkerhedsfunktionerne i programmet **Dell Data Protection | Adgang (Access)** administreres centralt for flere platforme, dvs. fjernadministration). I dette tilfælde kan Windows-sikkerhedsinfrastrukturen, f.eks. Active Directory, bruges til sikker administration af bestemte funktioner i **Dell Data Protection | Adgang (Access)**.

Når en computer fjernadministreres, dvs. "ejes" af fjernadministratoren, deaktiveres lokal administration af funktionaliteten i **Dell Data Protection | Adgang (Access)**. Administrationsvinduerne i programmet kan ikke åbnes lokalt. Følgende funktioner kan fjernadministreres:

- Trusted Platform Module (TPM)
- ControlVault
- Pre-Windows-logon
- Nulstilling af system
- BIOS -adgangskoder
- Windows-logonpolitik
- Self-Encrypting Drives
- Registrering af fingeraftryk og smartcard

Hvis du vil have flere oplysninger om brug af Wave Systems' EMBASSY® Remote Administration Server (ERAS) til fjernadministration, skal du kontakte din lokale Dell-forhandler eller gå til dell.com.

Indstillinger for adgang (Access Options)

I vinduet Indstillinger for adgang (Access Options) kan du angive, hvordan du vil have adgang til systemet.

Hvis du har angivet indstillinger for **Dell Data Protection | Adgang (Access)**, vises de på startsiden med de tilgængelige indstillinger, f.eks. indstillingen for ændring af adgangskode for Pre-Windows-logon. De tilgængelige indstillinger er genveje, som du kan klikke på for at gå til det relevante vindue og udføre en bestemt opgave, f.eks. ændre din Pre-Windows-adgangskode eller registrere et andet fingeraftryk.

Generelt
Som det første kan du angive, hvornår du vil logge på (Windows, Pre-Windows eller begge), og hvordan (f.eks. fingeraftryk og adgangskode) du vil logge på. Du kan vælge én eller to indstillinger for at logge på. De omfatter kombinationer af fingeraftryk, smartcard og adgangskode. De angivne indstillinger er baseret på de logonpolitikker, der gælder for miljøet, samt det, der understøttes på platformen.

Fingeraftryk
Hvis systemet indeholder en fingeraftrykslæser, kan du registrere eller opdatere fingeraftryk, du kan bruge til at logge på systemet. Når du har registreret fingeraftryk, kan du stryge den registrerede finger hen over systemets fingeraftrykslæser for at få adgang til systemet i Windows, Pre-Windows eller begge (afhængigt af, hvad du har angivet under Generelle indstillinger for adgang (General Access Options). Se Registrering af brugerfingeraftryk for at få flere oplysninger.

Pre-Windows-logon
Hvis du har angivet, at brugere skal logge på Pre-Windows, skal du oprette en systemadgangskode (også kaldet en Pre-Windows-adgangskode) til Pre-Windows-adgang. Når den er oprettet, kan administratoren når som helst ændre den.

Du kan også deaktivere Pre-Windows-logon fra denne skærm. For at gøre dette skal du indtaste din nuværende systemadgangskode, bekræfte, at adgangskoden er korrekt og derefter klikke på kappen **Deaktiver**.

Smartcard
Hvis du har angivet, at brugere skal bruge smartcard for at logge på, skal du registrere ét eller flere traditionelle (contacted) eller contactless smartcards. Klik på linket **Registrer endnu et smartcard** for at starte guiden til registrering af smartcard. Registrering betyder, at smartcardet indstilles til brug ved logon.

Når du har registreret et smartcard, kan du ændre eller oprette en PIN-kode til kortet vha. linket **Skift eller opret PIN-kode til smartcard** (Change or setup my smartcard PIN).

Pre-Windows-logon

Når Pre-Windows-logon er aktiveret, skal du angive godkendelse (adgangskode, fingeraftryk eller smartcard), når systemet startes, før Windows kan indlæses. Funktionaliteten til Pre-Windows-logon giver yderligere sikkerhed til systemet og holder uautoriserede brugere fra at åbne Windows og få adgang til computeren, f.eks. hvis den er blevet stjålet.

Fra vinduet Pre-Windows-logon (Pre-Windows Login) kan administratorer oprette Pre-Windows-logon eller oprette eller ændre en Pre-Windows (System) adgangskode. Hvis der allerede er angivet en adgangskode, kan du deaktivere Pre-Windows-logon fra dette vindue. Ved oprettelse af Pre-Windows-logon startes en guide, der udfører følgende:

- Systemadgangskode: Opret en systemadgangskode (også kaldet en Pre-Windows-adgangskode) til Pre-Windows-adgang. Denne adgangskode bruges også som sikkerhedskopi, hvis en bruger har flere godkendelsesfaktorer, f.eks. for at få adgang til systemet, hvis der er problemer med fingeraftrykssensoren.
- Fingeraftryk eller smartcard: Opret et fingeraftryk eller smartcard til brug ved Pre-Windows-logon, og angiv, om denne godkendelsesfaktor skal bruges i stedet for eller sammen med Pre-Windows-adgangskoden.
- Single Sign On: Som standard bliver din Pre-Windows-godkendelse (adgangskode, fingeraftryk eller smartcard) brugt til automatisk også at logge på Windows - det kaldes "Single Sign On". Hvis du vil deaktivere denne funktion, skal du markere afkrydsningsfeltet "Jeg vil logge på igen i Windows" (I want to login again at Windows).
- Hvis der er oprette en BIOS -harddiskadgangskode udover en Pre-Windows-adgangskode, har du også mulighed for at ændre eller deaktivere harddiskadgangskoden.

BEMÆRK: Ikke alle fingeraftrykslæsere kan bruges til Pre-Windows-godkendelse. Hvis din læser ikke er kompatibel, kan du kun registrere fingeraftryk til Windows-logon. Hvis du vil vide, om en bestemt fingeraftrykslæser er kompatibel, skal du kontakte systemadministratoren eller gå til support.dell.com for at se en liste over understøttede fingeraftrykslæsere.

Deaktiver Pre-Windows-logon
Du kan også deaktivere Pre-Windows-logon fra dette vindue. For at gøre dette skal du indtaste din nuværende Pre-Windows (system) adgangskode, bekræfte, at adgangskoden er korrekt og derefter klikke på kappen **Deaktiver**. Bemærk, at hvis du deaktiverer Pre-Windows-logon, er alle registrerede fingeraftryk eller smartcards stadig registrerede.

Registrering/fjernelse af fingeraftryk

Brugere kan registrere eller opdatere fingeraftryk, som kan bruges til godkendelse i systemet i forbindelse med Pre-Windows- eller Windows-logon. Under fanen Fingeraftryk (Fingerprint) kan du se, hvilke fingre, der er registreret. Hvis du klikker på linket **Registrer endnu en finger** (Enroll another), startes guiden Registrering af fingeraftryk (Fingerprint Enrollment), der fører dig gennem registreringsprocessen. "Registrere" betyder, at et fingeraftryk gemmes, så det kan bruges til logon. Der skal være en gyldig fingeraftrykslæser installeret og konfigureret for at du kan registrere fingeraftryk.

BEMÆRK: Ikke alle fingeraftrykslæsere kan bruges til Pre-Windows-logon. Der vises en fejlmeddelelse, hvis du forsøger at registrere til Pre-Windows med en inkompatibel læser. Hvis du vil vide, om en bestemt enhed er kompatibel, skal du kontakte systemadministratoren eller gå til support.dell.com for at se en liste over understøttede fingeraftrykslæsere.

Når du registrerer fingeraftryk, bliver du bedt om at angive din Windows-adgangskode for at bekræfte din identitet. Hvis politikken kræver det, bliver du også bedt om at angive din Pre-Windows (System) -adgangskode. Pre-Windows-adgangskoden kan bruges til at få adgang til systemet, hvis der er problemer med fingeraftrykslæseren.

NOTER:

- Det anbefales, at du registrerer mindst to fingeraftryk under tilmeldingsprocessen.
- Du skal sikre, at fingeraftryk er registreret korrekt, inden mulighederne for fingeraftryksgodkendelse aktiveres.
- Hvis du skifter fingeraftrykslæsere på systemet, skal du registrere fingeraftryk igen med den nye læser. Det anbefales ikke, at skifte frem og tilbage mellem to forskellige fingeraftrykslæsere.
- Hvis du gentagne gange får vist meddelelsen "Sensoren mistede fokus" (sensor lost focus) ved registrering af fingeraftryk, kan det betyde, at computeren ikke genkender fingeraftrykslæseren. Hvis fingeraftrykslæseren er ekstern, kan problemet ofte løses ved at frakoble den og derefter tilslutte den igen.

Sletning af registrerede fingeraftryk

Du kan fjerne registrerede fingeraftryk ved at klikke på linket **Fjern fingeraftryk** (Remove fingerprint) eller ved at klikke (for at fjerne markeringen) på en registreret finger i guiden Registrering af fingeraftryk (Fingerprint Enrollment).

Hvis du vil fjerne en bestemt bruger, som har registreret fingeraftryk til Pre-Windows-godkendelse, kan administratoren fjerne alle fingeraftryk, der er registreret for denne bruger.

BEMÆRK: Hvis der opstår andre fejl under registrering af fingeraftryk, kan du gå til wave.com/support/Dell for at få flere oplysninger.

Registrering smartcard

I **Dell Data Protection | Adgang (Access)** har du mulighed for at bruge et traditionelt (contacted) eller contactless smartcard til at logge på din Windows-konto eller til Pre-Windows-godkendelse. Under fanen Smartcard skal du klikke på linket **Registrer endnu et smartcard** (Enroll another smartcard) for at starte Smartcard Enrollment wizard, der guider dig gennem registreringsprocessen. "Registrere" betyder, at smartcardet indstilles til brug ved logon.

Du skal have en gyldig smartcard-godkendelsesenhed installeret og konfigureret for at kunne udføre registrering.

BEMÆRK: Hvis du vil vide, om en bestemt enhed er kompatibel, skal du kontakte systemadministratoren eller gå til support.dell.com for at se en liste over understøttede smartcards.

Registrering
Når du registrerer et smartcard, bliver du bedt om at angive din Windows-adgangskode for at bekræfte din identitet. Hvis politikken kræver det, bliver du også bedt om at angive din Pre-Windows (System) -adgangskode. Pre-Windows-adgangskoden kan bruges til at få adgang til systemet, hvis der er problemer med smartcard-læseren.

Under registreringen bliver du bedt om at angive smartcard-PIN-koden, hvis der findes en. Hvis politikken kræver en PIN -kode, og der ikke er angivet en, bliver du bedt om at oprette en.

NOTER:

- Når en bruger er registreret til at bruge smartcard i Pre-Windows, kan vedkommende ikke fjernes.
- Standardbrugere kan ændre bruger-PIN -koden på et smartcard, og administratoren kan ændre både administrator-PIN -koden og bruger-PIN-koden.
- Administratoren kan også nulstille et smartcard. Når det er nulstillet, kan smartcardet ikke bruges til godkendelse ved Windows-logon eller til Pre-Windows, før det er registreret igen.

BEMÆRK:I forbindelse med godkendelse af TPM-certifikater kan administratorer registrere TPM-certifikater vha. Microsoft Windows-processen til registrering af smartcard. Administratorer skal vælge "Wave TCG-Enabled CSP" som Cryptographic Service Provider i stedet for Smartcard CSP for at opnå kompatibilitet med dette program. Derudover skal Dell sikker logon (Dell Secure login) være aktiveret med den relevante godkendelsestypepolitik for klienten.

BEMÆRK: Hvis du får vist en fejlmeddelelse om, at Smartcard-tjenesten ikke kører, kan du starte/genstarte tjenesten på følgende måde:

- Klik på Administration (Administrative Tools) i Kontrolpanel, vælg Tjeneste (Service), højreklik på Smartcard, og vælg derefter Start eller Genstart (Restart).
- Hvis du vil have flere oplysninger om en bestemt fejlmeddelelse, skal du gå til wave.com/support/Dell.

Self-Encrypting Drive

Dell Data Protection | Adgang (Access)administrerer de hardwarebaserede sikkerhedsfunktioner for self-encrypting drives, som har datakryptering integreret i drevhardwaren. Denne funktionalitet sikrer, at kun godkendte brugere kan få adgang til krypterede data, når drevlåsning er aktiveret.

Vinduet Self-Encrypting Drive åbnes ved at klikke på **Self-Encrypting Drive**. Denne fane vises kun, hvis systemet indeholder ét eller flere SED'er.

Klik på linket **Opsætning** (Setup) for at starte guiden Self-Encrypting Drive. I denne guide kan du oprette en drevadministratoradgangskode, sikkerhedskopiere adgangskoden og anvende indstillingerne for drevkryptering. Kun systemadministratorer kan åbne guiden Self-Encrypting Drive.

Vigtigt! Når drevet er oprettet, aktiveres databeskyttelse og drevlåsning. Når et drev er låst, sker følgende:

- Drevet går i *låst* tilstand, når strømmen til drevet slukkes.
- Drevet starter ikke, med mindre brugeren indtaster korrekt brugernavn og adgangskode (eller fingeraftryk) på Pre-Windows-logonskærmen. Før drevlåsning er aktiveret, er dataene på drevet tilgængelige for alle brugere på computeren.
- Drevet er sikret, selvom det er tilkoblet en anden computer som et sekundært drev. Det kræver godkendelse af få adgang til drevdata.

Når drevet er oprettet, viser vinduet Self-Encrypting Drive drevene og et link til brugere om at ændre deres adgangskoder. Hvis du er drevadministrator, kan du desuden tilføje eller fjerne drevbrugere fra dette vindue. Hvis der er oprettet et eksternt drev, vises det i dette vindue, og det kan låses op.

BEMÆRK: Hvis du vil låse et sekundært, eksternt drev op, skal drevet være slukket uafhængigt af computeren.

Drevadministratoren kan administrere drevindstillinger i **Avancerede>enheder** (Advanced Devices). Du kan finde flere oplysninger i Enhedshåndtering (Device Management) - Self-Encrypting Drives.

Opsætning af drev

Guiden Self-Encrypting Drive fører dig gennem opsætning af drev. Følgende er vigtigt at huske i forbindelse med denne proces.

Drevadministrator
Den første bruger med systemadministratorrettigheder, der opretter drevadgang (og angiver adgangskoden for drevadministrator) bliver drevadministrator. Det er den eneste bruger, der har tilstrækkelige rettigheder til at foretage ændringer for drevadgang. For at sikre, at den første bruger er den 'korrekte' drevadministrator, skal du markere afkrydsningsfeltet "Jeg forstår" (I understand) for at kunne fortsætte.

Drevadministrator adgangskode
Guiden beder dig om at oprette en drevadministratoradgangskode og indtaste den igen for at bekræfte den. Du skal indtaste din Windows-adgangskode for at identificere dig selv, før du kan oprette din drevadministratoradgangskode. Den aktuelle Windows-bruger skal have administratorrettigheder for at kunne oprette adgangskoden.

Sikkerhedskopiering af drevlegitimationsoplysninger
Angiv en placering, eller klik på knappen **Gennemse** for at vælge en placering, for at gemme en sikkerhedskopi af dine drevadministratorlegitimationsoplysninger.

VIGTIGT**!**

- Det anbefales på det kraftigste, at du sikkerhedskopierer disse legitimationsoplysninger, og at du sikkerhedskopierer dem til et andet drev end din primære harddisk (f.eks. flytbare medier). Ellers kan du risikere, at du ikke kan få adgang til din sikkerhedskopi, hvis du mister adgang til drevet.
- Når du har oprettet drevet, skal allebrugere indtaste korrekt brugernavn og adgangskode (eller fingeraftryk) før Windows indlæses, for at kunne få adgang til systemet, næste gang systemet startes.

Tilføj drevbruger
Drevadministratoren kan tilføje andre brugere til drevet, som er gyldige Windows-brugere. Når administratoren tilføjer brugere til drevet, har vedkommende mulighed for at kræve, at brugeren nulstiller sin adgangskode, første gang der logges på. Brugeren bliver bedt om at nulstille sin adgangskode på Pre-Windows-godkendelsesskærmen, før drevet låses op.

Avancerede indstillinger

- *Single Sign On* - Som standard bruges din Self-Encrypting Drive-adgangskode, som du indtaster i Pre-Windows for at godkende drevet, til automatisk at logge på Windows også (kaldet "Single Sign On"). Hvis du vil deaktivere denne funktion, skal du markere "Jeg vil logge på igen, når Windows starter (I want to login again when Windows starts), når du konfigurerer drevindstillingerne.
- *Logon med fingeraftryk* - På understøttede platforme kan du angive, at du vil godkendes over for SED vha. fingeraftryk i stedet for en adgangskode.
- *Sleep/Standby (S3) Support* (hvis understøttet på platform) - Hvis aktiveret, kan dit SED sættes sikkert i slumre/dvaletilstand (også kaldet S3-tilstand) og kræver Pre-Windows-godkendelse for at genoptage fra slumre/dvaletilstand.

NOTER:

- Når S3 Support er aktiveret, er drevkrypteringsadgangskoder underlagt eventuelle BIOS - adgangskodebegrænsninger. Kontakt producenten af systemhardwaren for flere oplysninger om specifikke BIOS-adgangskodebegrænsninger, der måtte være på systemet.
- Ikke alle SED'er understøtter S3-tilstand. Under opsætning af drev får du besked om, om drevet understøtter slumre/dvaletilstand. I forbindelse med drev, der ikke understøtter denne tilstand, konverteres Windows S3-anmodninger automatisk til dvaleanmodninger, hvis dvaletilstand er aktiveret (det anbefales på det kraftigste, at du aktiverer dvaletilstand på computeren).
- Første gang du logger på efter indstilling af Single Sign On (SSO) , stopper processen midlertidigt ved Windows-logonprompten. Du bliver bedt om at indtaste din form for Windows-godkendelse, der lagres sikkert til fremtidige forsøg på Windows-logon. Næste gang systemet startes, logger SSO dig automatisk på Windows. Samme proces kræves også, hvis en brugers Windows-godkendelse (adgangskode, fingeraftryk, smartcard-PIN-kode) ændres. Hvis computeren er i et domæne, og domænet har en politik, der kræver, at der trykkes på ctrl+alt+del for Windows-logon, overholdes denne politik.

ADVARSEL! Hvis du fjerner programmet **Dell Data Protection | Adgang (Access)**, skal du først deaktivere SED-databeskyttelse og låse drevet op.

Self-Encrypting Drive - brugerfunktioner

SED-administratorer (self-encrypting drive) udfører al administration af drevsikkerhed og brugere. Drevbrugere, som ikke er drevadministratorer, kan kun udføre følgende opgaver:

- Ændre deres egen drevadgangskode
- Låse et drev op

Disse opgaver kan åbnes fra fanen **Self-Encrypting Drive** i **Dell Data Protection | Adgang (Access)**.

Skift adgangskode
Dette gør det muligt for registrerede brugere at oprette en ny godkendelsesadgangskode. Du skal angive din aktuelle Self-Encrypting Drive-adgangskode, før drevadgangskoden indstilles til en ny værdi.

NOTER:

- Programmet gennemtvinger Windows-adgangskodens længde og Windows-adgangskodens kompleksitetspolitikker, hvis disse er aktiveret. Hvis Windows-adgangskodepolitikker ikke er aktiveret, er den største længde for en Self-Encrypting Drive-adgangskode 32 tegn. Bemærk, at den maksimale længde er 127 tegn, hvis S3 (Sleep/Standby) ikke er aktiveret.
- En brugers SED-adgangskode er forskellig fra Windows-adgangskoden. Når en brugers Windows-adgangskode ændres eller nulstilles, påvirker det ikke brugerens drevadgangskode, med mindre Windows Synkronisering af adgangskoder er aktiveret. Se Enheder: Self-Encrypting Drives for at få flere oplysninger.
- På nogle ikke-engelske tastaturer findes der er sæt begrænsede tegn, der ikke kan bruges til SED-adgangskoden. Hvis Windows-adgangskoden indeholder nogle af de begrænsede tegn, og Windows Synkronisering af adgangskoder er aktiveret, mislykkes synkroniseringen, hvilket resulterer i en fejlmeddelelse.

Lås drev op
Oplåsning af drev giver en registreret drevbruger mulighed for at låse et låst drev op. Hvis drevlåsning er aktiveret, går drevet i låst tilstand, når som helst der slukkes for strømmen til pc'en. Når systemet startes igen, skal du angive godkendelse for drevet ved at indtaste din adgangskode på godkendelsesskærmen i Pre-Windows.

NOTER:

- Computeren kan muligvis ikke gå i strømbesparende tilstand, dvs. slumre eller dvale, hvis der er aktiveret flere forskellige SED-brugerkonti på computeren på samme tid.
- På Pre-Windows-godkendelsesskærmbilledet erstatter Bruger 1, Bruger 2 osv. drevbrugernavne i versioner af programmet, der er lokaliseret til følgende sprog: Kinesisk, Japansk, Koreansk og Russisk.

Avancerede indstillinger (Advanced Options)

De avancerede indstillinger i **Dell Data Protection | Adgang (Access)** giver en bruger med administratorrettigheder mulighed for at administrere følgende områder i programmet:

Vedligeholdelse
Adgangskoder
Enheder

BEMÆRK: Det er kun brugere med administratorrettigheder, som kan foretage ændringer i de avancerede indstillinger. Standardbrugere kan få vist disse indstillinger, men de kan ikke ændre dem.

Vedligeholdelse (Maintenance)

Administratorer kan bruge vinduet Vedligeholdelse (Maintenance) til at angive Windows-logonpræferencer, til at nulstille systemet til anden brug eller til at gemme eller gendanne legitimationsoplysninger, der er gemt i systemets sikkerhedshardware. Se følgende emner for at få flere oplysninger:

Adgangspræferencer
Nulstilling af system
Arkivering og gendannelse af & legitimationsoplysninger (Credential Archive Restore)

Adgangspræferencer

I vinduet Adgangspræferencer (Access Preferences) kan administratorer angive indstillinger for Windows-logon for alle brugere på systemet.

Aktiver Dell sikker logon (Enable Dell Secure Login)
Med indstillingen for erstatning af standard Windows ctrl-alt-delete-skærmen kan du bruge forskellige godkendelsesfaktorer i stedet for (eller udover) Windows-adgangskoden for at få adgang til Windows. Du kan vælge at tilføje et fingeraftryk som en anden godkendelsesfaktor for at styrke sikkerheden i Windows-logonprocessen. Du kan også tilføje yderligere godkendelsesfaktorer for Windows-logon, herunder et smartcard eller TPM-certifikat.

NOTER:

- Aktivering af Dell sikker logon påvirker alle brugere på systemet.
- Det anbefales, at indstillingen aktiveres EFTER at brugere har registreret deres fingeraftryk eller smartcard.
- Første gang du logger på, efter at denne indstilling er angivet, bliver du bedt om at bekræfte over for Windows i henhold til standardpolitikken, og derefter skal du bruge de nye godkendelsesfaktorer ved næste start.

Deaktiver Dell sikker logon (Disable Dell Secure login)
Denne indstilling deaktiverer alle **Dell Data Protection | Adgang (Access)**-funktioner til Windows-logon. Hvis denne indstilling er valgt, nulstilles til standard Windows-logonpolitikken.

NOTER:

- Hvis du får vist en fejl om sikker Windows-logon, når du prøver at logge på, skal du deaktivere og derefter genaktivere indstillingen Dell sikker logon (Dell Secure login).
- Hvis du vil have flere oplysninger om en bestemt fejlmeddelelse, skal du gå til wave.com/support/Dell.

Nulstilling af system

Funktionen til nulstilling af systemet bruges til at slette alle brugerdata fra al sikkerhedshardware på platformen, f.eks. hvis computeren skal bruges til et andet formål. Indstillingen sletter alle adgangskoder på systemet med undtagelse af Windows-brugeradgangskoder, samt alle data på hardwareenheder, f.eks. ControlVault, TPM og fingeraftrykslæsere. I forbindelse med selvkrypterende drev deaktiverer funktionen desuden databeskyttelse, så drevdataene bliver tilgængelige.

Du skal bekræfte, at du er klar over, at du nulstiller systemet, og derefter skal du klikke på **Næste**. Hvis du vil nulstille systemet, skal du angive en adgangskode for hver sikkerhedsenhed, hvis disse er oprettet:

- TPM -ejer
- ControlVault Administrator
- BIOS Administrator
- BIOS System (pre-Windows)
- Harddisk (BIOS)
- Self-Encrypting Drive Administrator

BEMÆRK: I forbindelse med selvkrypterende drev er det kun nødvendigt at angive adgangskoden for drevadministratoren.

Vigtigt! Den eneste måde du kan gendanne de data, du sletter, når systemet nulstilles, er ved at gendanne fra et tidligere gemt arkiv. Hvis du ikke har et arkiv, kan dataene ikke gendannes. I forbindelse med et selvkrypterende drev er det kun opsætningsdataene, der slettes. Der slettes ingen personlige data på drevet.

Arkivering og gendannelse af &legitimationsoplysninger (Credential Archive Restore)

Funktionen til arkivering og gendannelse af legitimationsoplysninger bruges til at sikkerhedskopiere og gendanne alle brugerlegitimationsoplysninger (logon- og krypteringsoplysninger), som er gemt i ControlVault og Trusted Platform Module (TPM). Det er vigtigt at sikkerhedskopiere disse data ved køb af ny computer eller til gendannelse af data, hvis der opstår hardwarefejl. Her er det muligt at gendanne alle dine legitimationsoplysninger til den nye computer fra en gemt arkivfil.

Du kan vælge at arkivere eller gendanne legitimationsoplysninger for en enkelt bruger eller for alle brugere på systemet.

Brugerlegitimationsoplysningerne består af data, der bruges i Pre-Windows, f.eks. registrerede fingeraftryk og smartcarddata samt nøgler, der er gemt i TPM. TPM opretter nøgler efter anmodning fra sikre programmer, f.eks. vil oprettelse af et digitalt certifikat oprette nøgler i TPM.

BEMÆRK: For at afgøre om TPM-nøglerne kan arkiveres med **Dell Data Protection | Adgang (Access)**, skal du læse dokumentationen til det sikre program.. Generelt understøttes programmer, der anvender "Wave TCG-Enabled CSP" til at oprette nøgler.

Arkivering af legitimationsoplysninger
Hvis du vil gemme legitimationsoplysninger, skal du gøre følgende:

- Angiv, om du gemmer legitimationsoplysninger for dig selv eller for alle brugere på systemet.
- Angiv bekræftelse for sikkerhedshardwaren ved at indtaste system (Pre-Windows) adgangskoden, ControlVault-administratoradgangskoden og TPM - ejeradgangskoden.
- Opret en adgangskode for sikkerhedskopiering af legitimationsoplysninger.
- Angiv en placering vha. knappen **Gennemse** (Browse). Arkivplaceringen skal være på et flytbart medie, f.eks. en USB-nøgle eller et netværksdrev, for at sikre, at den ikke går tabt, hvis der opstår harddiskfejl.

Vigtig bemærkning:

- Husk placeringen, da brugeren skal bruge disse oplysninger til at gendanne legitimationsoplysningerne.
- Husk adgangskoden til sikkerhedskopien af legitimationsoplysningerne for at sikre, at dataene kan gendannes. Det er meget vigtigt, fordi denne adgangskode ikke kan gendannes.
- Hvis du ikke kender TPM-ejeradgangskoden, skal du kontakte systemadministratoren eller læse TPM-installationsvejledningen for pc'en.

Gendannelse af legitimationsoplysninger
Hvis du vil gendanne legitimationsoplysninger, skal du gøre følgende:

- Angiv, om du gendanner legitimationsoplysninger for dig selv eller for alle brugere på systemet.
- Gå til den relevante placering, og vælg arkivfilen.
- Indtast den adgangskode for sikkerhedskopiering af legitimationsoplysninger, der blev oprettet, dat du oprettede arkivet.
- Angiv bekræftelse for sikkerhedshardwaren ved at indtaste system (Pre-Windows) adgangskoden, ControlVault-administratoradgangskoden og TPM - ejeradgangskoden.

NOTER:

- Hvis du får vist en fejl om, at legitimationsoplysningerne ikke er blevet gendannet, og du har prøvet at udføre gendannelsen flere gange, kan du prøve at gendanne en anden arkivfil. Hvis det ikke lykkes, skal du oprette et nyt arkiv og prøve at gendanne fra dette arkiv.
- Hvis du får vist en fejlmeddelelse om, at TPM -nøglerne ikke kunne gendannes, skal du oprette et legitimationsoplysningsarkiv og derefter fjerne TPM i BIOS. slet TPM, genstart computeren, tryk på **F2**, når sikkerhedskopieringen starter for at få adgang til BIOS - indstillingerne, og gå derefter til Sikkerhed>TPM Sikkehed. Genetabler derefter ejerskabet over TPM, og prøv at gendanne legitimationsoplysningerne.
- Hvis du vil have flere oplysninger om en bestemt fejlmeddelelse, skal du gå til wave.com/support/Dell.

Administration af adgangskoder (Password Management)

Fra vinduet Administration af adgangskoder (Password Management) kan en administrator oprette eller ændre alle sikkerhedsadgangskoder på systemet:

- System (også kaldet Pre-Windows)*
- Administrator*
- Harddisk*
- ControlVault
- TPM -ejer
- TPM Master
- TPM -adgangskodeboks
- Self-Encrypting Drive

NOTER:

- Du får kun vist de adgangskoder, der er relevante for den aktuelle platformskonfiguration, så vinduet forandres på baggrund af systemkonfiguration og status.
- Adgangskoder med * ved siden af er BIOS-adgangskoder, og de kan også ændres i system-BIOS.
- Adgangskoder på BIOS-niveau kan ikke oprettes eller ændres, hvis BIOS-administratoren har afvist ændring af adgangskoder.
- Hvis du klikker på linket **opsætning** (setup) for et selvkrypterende drev, startes guiden Self-Encrypting Drive. Hvis du klikker på **administrer** (manage), kan en bruger ændre én eller flere Self-Encrypting Drive-adgangskoder.
- Hvis du klikker på linket **administrer** (manage) for TPM-adgangskodeboksen, vises et vindue, hvor du kan få vist og ændre de adgangskoder, der beskytter dine TPM-nøgler. Når du opretter en TPM-nøgle, der kræver en adgangskode, genereres adgangskoden vilkårligt og placeres i boksen. Du kan ikke administrere TPM-adgangskodeboksen, før du har oprettet en TPM-masteradgangskode.

Windows-adgangskode Regler for kompleksitet

Dell Data Protection | Adgang (Access) sikrer, at følgende adgangskoder overholder Windows regler for adgangskodekompleksitet for maskinen:

- TPM-ejeradgangskode

Sådan bestemmes Windows-adgangskodens kompleksitetspolitikker ved at følge disse trin:

1. Åbn Kontrolpanel.
2. Dobbeltklik på Administration.
3. Dobbeltklik på Lokal sikkerhedspolitik.
4. Udvid kontopolitikker og vælg Adgangskodepolitik.

Enheder (Devices)

Administratorer bruger vinduet Enheder (Devices) til at styre alle de sikkerhedsenheder, der er installeret på systemet. For hver enkelt enhed kan du få vist status og yderligere detaljerede oplysninger, f.eks. firmwareversion. Klik på **vis** (show) for at få vist oplysninger for en enhed, eller klik på **skjul** (hide) for at skjule. Følgende enheder kan administreres (afhængigt af platform):

Trusted Platform Module (TPM)
ControlVault®
Self-Encrypting Drive(s)
Oplysninger om godkendelsesenhed (Authentication Device Information)

Trusted Platform Module (TPM)

TPM-sikkerhedschippen skal aktiveres, og der skal angives ejerskab af TPM for at du kan bruge de avancerede sikkerhedsfunktioner i **Dell Data Protection | Adgang (Access)** og TPM.

Vinduet Trusted Platform Module i **Enhedshåndtering** (Device Management) vises kun, når et TPM er registreret i systemet.

TPM-administration

Disse funktioner giver systemadministratoren mulighed for at styre TPM.

Status

Viser status *aktiv* eller *inaktiv* for TPM. Status Aktiv betyder, at TPM er aktiveret i BIOS og er klar til opsætning (dvs. tildeling af ejerskab). TPM kan ikke administreres, og sikkerhedsfunktionerne kan ikke åbnes, hvis TPM ikke er aktiv (aktiveret).

Hvis TPM er registreret på systemet, men ikke er aktiveret, kan du aktivere det ved at klikke på linket **aktiver** i dette vindue uden at skulle åbne system-BIOS. Efter aktivering af TPM vha. denne funktion, skal computeren genstartes. Under genstarten får du muligvis vist en prompt, hvor du bliver bedt om at acceptere ændringerne.

BEMÆRK: Muligheden for at aktivere TPM fra dette program understøttes måske ikke på alle platforme. Hvis det ikke understøttes, skal du aktivere det i systemets BIOS. For at gøre dette skal du genstarte systemet, trykke på **F2**, før Windows indlæses for at åbne BIOS . Derefter skal du gå til Sikkerhed (Security)>TPM Sikkerhed (Security) og aktivere TPM.

Du kan også *deaktivere* TPM herfra ved at klikke på linket **deaktiver**. Hvis du deaktiverer TPM , er det ikke tilgængeligt for de avancerede sikkerhedsfunktioner. Deaktivering ændrer dog ingen TPM-indstillinger eller sletter eller ændrer oplysninger eller nøgler i TPM.

Ejet

Viser status for ejerskab (f.eks. "ejet") og giver dig mulighed for at oprette eller ændre TPM -ejer. TPM -ejerskab skal angives for at sikkerhedsfunktionerne kan anvendes. Før ejerskabet kan angives, skal TPM aktiveres.

Processen for angivelse af ejerskab indebærer, at brugeren (med administratorrettigheder) opretter en TPM-ejeradgangskode. Når denne adgangskode er defineret, er ejerskab defineret, og TPM er klar til brug.

BEMÆRK: TPM -ejeradgangskoden skal overholde Regler for Windows-adgangskodes kompleksitet for systemet.

Vigtigt! Det er vigtigt, at du ikke mister eller glemmer TPM -ejeradgangskoden, da den skal brugestil at få adgang til de avancerede sikkerhedsfunktioner for TPM i **Dell Data Protection | Adgang (Access)**.

Låst

Viser status *låst* eller *låst op* for TPM. "Låsning" er en sikkerhedsfunktion i TPM. TPM går i låst tilstand, efter et bestemt antal mislykkede forsøg på at indtaste den korrekte TPM -ejeradgangskode. TPM -ejeren kan låse TPM op herfra. TPM -ejeradgangskoden skal angives.

NOTER:

- Hvis du får vist en fejlmeddelelse om, at TPM -ejerskabet ikke kunne fastslås, skal du slette TPM i system-BIOS og prøve at angive ejerskabet igen. Hvis du vil slette TPM, skal

du genstarte computeren, trykke på **F2** for at få adgang til BIOS -indstillingerne og derefter gå til Sikkerhed (Security)>TPM Sikkerhed (Security).

- Hvis du får vist en fejlmeddelelse om, at TPM -ejeradgangskoden ikke kunne ændres, skal du gemme TPM -dataene (legitimationsoplysningsarkiv), slette TPM i BIOS, angive ejerskab af TPM igen og gendanne TPM -data (gendan legitimationsoplysninger).
- Hvis du vil have flere oplysninger om en bestemt fejlmeddelelse, skal du gå til wave.com/support/Dell.

Dell ControlVault®

Dell ControlVault® (CV) er et sikkert hardwarelager til brugerlegitimationsoplysninger, der bruges ved Pre-Windows-logon, f.eks. brugeradgangskoder eller registrerede fingeraftryksdata. Vinduet ControlVault i **Enhedshåndtering** (Device Management) vises kun, når et ControlVault er registreret i systemet.

ControlVault Management

Disse funktioner giver systemadministratoren mulighed for at styre systemets ControlVault.

Status
Viser status *aktiv* eller *inaktiv* for ControlVault. Statussen "Inaktiv" betyder, at ControlVault ikke er tilgængelig for lagring på systemet. Se Dell-systemdokumentationen for at finde frem til, om systemet indeholder en ControlVault.

Adgangskode (Password)
Angiver, om der er angivet en ControlVault-administratoradgangskode, og du kan oprette en adgangskode eller ændre en adgangskode (hvis der allerede er oprettet en). Kun systemadministratorer kan oprette eller ændre denne adgangskode. Der skal være angivet en ControlVault-administratoradgangskode for at:

- arkivere eller gendanne legitimationsoplysninger.
- slette brugerdata (for alle brugere).

BEMÆRK: Hvis der udføres forsøg på en arkivering eller gendannelse, mens ControlVault-administratoradgangskoden ikke er angivet, bliver man bedt om at oprette en (hvis man er administrator).

Registrerede brugere (Enrolled Users)
Angiver, om brugere har registreret logonlegitimationsoplysninger, f.eks. adgangskoder, fingeraftryk eller smartcard-data, som aktuelt lagres i ControlVault.

Slet brugerdata
Det kan være nødvendigt at slette dataene i ControlVault på et tidspunkt, f.eks. hvis brugere har problemer med at bruge eller registrere Pre-Windows-legitimationsoplysninger. Alle data, der er gemt i ControlVault, kan slettes fra dette vindue - både for en enkelt bruger og for alle brugere.

ControlVault-administratoradgangskoden skal indtastes for at slette alle brugerdata på platformen. Du bliver også bedt om at angive systemadgangskoden (Pre-Windows) , hvis der er registreret Pre-Windows-legitimationsoplysninger. Hvis du sletter alle brugerdata, nulstilles ControlVault-administratoradgangskoden og systemadgangskoden. Bemærk, at dette er den eneste måde at slette ControlVault-administratoradgangskoden på.

BEMÆRK: Når du har slettet alle brugerdata, bliver du bedt om at genstarte computeren. Det er vigtigt, at du genstarter computeren for at sikre, at systemet fungerer korrekt.

ControlVault-administratoradgangskoden skal ikke angives for at slette en enkelt brugers legitimationsoplysninger. Når du klikker på **slet brugerdata** (clear user data), bliver du bedt om at vælge den bruger, hvis ControlVault-legitimationsoplysninger der skal slettes. Når du har valgt en bruger, bliver du bedt om at angive systemadgangskoden (kun, hvis der er registreret Pre-Windows-legitimationsoplysninger).

NOTER:

- Hvis du får vist en fejlmeddelelse om, at ControlVault-administratoradgangskoden ikke kan oprettes, skal du gemme dine legitimationsoplysninger, slette alle brugerdata fra ControlVault, genstarte computeren og forsøge at oprette adgangskoden igen.
- Hvis du får vist en fejlmeddelelse om, at legitimationsoplysningerne ikke kunne slettes fra ControlVault for en enkelt bruger, skal du arkivere dine legitimationsoplysninger, prøve at slette alle brugerdata og derefter prøve at slette dataene for den enkelte bruger igen.
- Hvis du får vist en fejlmeddelelse om, at legitimationsoplysninger ikke kunne slettes fra ControlVault for alle brugere, skal du overveje at nulstille systemet. **Vigtigt!** Læs hjælpemnet om nulstilling af systemet, før du nulstiller, da en nulstilling vil slette ALLE brugersikkerhedsdata.
- Hvis du får vist en fejlmeddelelse om, at ControlVault- og TPM -data ikke kan sikkerhedskopieres, skal du deaktivere TPM i systemets BIOS. Det gør du ved at genstarte computeren, trykke på **F2**, når sikkerhedskopieringen starter for at få adgang til BIOS-indstillingerne, og derefter gå til Sikkerhed>TPM Sikkerhed. Genaktiver derefter TPM , og prøv at arkivere dine ControlVault-data igen.
- Hvis du vil have flere oplysninger om en bestemt fejlmeddelelse, skal du gå til wave.com/support/Dell.

Self-Encrypting Drives: Avanceret

Dell Data Protection | Adgang (Access) administrerer de hardwarebaserede sikkerhedsfunktioner for self-encrypting drives, som har datakryptering integreret i drevhardwaren. Administrationen sikrer, at kun godkendte brugere kan få adgang til krypterede data, når drevlåsning er aktiveret.

Vinduet Self-Encrypting Drive i **Enhedshåndtering** (Device Management) vises kun, hvis der findes én eller flere SED'er på systemet.

Vigtigt! Når drevet er oprettet, aktiveres SED-databeskyttelse og drevlåsning.

Drevadministration (Drive Management)
Disse funktioner giver drevadministratoren mulighed for at administrere indstillingerne for drevsikkerhed. Ændringer i indstillingerne for drevsikkerhed træder i kraft, når drevet har været slukket.

Databeskyttelse (Data Protection)
Viser status *aktiveret* eller *deaktiveret* for SED-databeskyttelse. Status 'aktiveret' betyder, at drevsikkerheden er oprettet, men så længe *låsning* af drev er aktiveret, skal brugere ikke godkendes Pre-Windows for at åbne drev.

Du kan deaktivere SED-databeskyttelse her. Når det er deaktiveret, slås alle avancerede sikkerhedsfunktioner for SED fra, og drevet fungerer som et standarddrev. Hvis du deaktiverer databeskyttelse, slettes alle sikkerhedsindstillinger, herunder legitimationsoplysninger for drevadministratorer og drevbrugere. Denne funktion ændrer eller sletter dog ikke brugerdata på drevet.

Låsning (Locking)
Viser status *aktiveret* eller *deaktiveret* for self-encrypting drive(s). Se emnet Self-Encrypting Drive for at få oplysninger om låste drev.

Det kan være nødvendigt midlertidigt at deaktivere drevlåsning, hvilket du kan gøre herfra. Det anbefales dog ikke, da der ikke skal angives legitimationsoplysninger for at åbne drevet, når drevlåsning er deaktiveret, så alle platformbrugere har adgang til drevdata. Deaktivering af drevlåsning sletterikke nogen sikkerhedsindstillinger, herunder legitimationsoplysningerne for drevadministratoren og drevbrugerne eller nogen data på drevet.

ADVARSEL!Hvis du fjerner programmet **Dell Data Protection | Adgang (Access)**, skal du først deaktivere SED-databeskyttelse og låse drevet op.

Drevadministrator (Drive Administrator)

Viser den aktuelle drevadministrator. Herfra kan drevadministratoren ændre, hvem der er drevadministrator. Den nye administrator skal være en gyldig Windows-bruger på systemet med administratorrettigheder. Der kan kun være én drevadministrator på systemet.

Drevbrugere (Drive Users)

Viser de registrerede drevbrugere og antallet af aktuelt registrerede brugere. Det maksimale antal understøttede brugere er baseret på det selvkrypterende drev (aktuelt 4 brugere for Seagate-drev og 24 for Samsung-drev).

Windows-adgangskode Sync
Funktionen WPS (Windows password synchronization) indstiller automatisk en brugers Self-Encrypting Drive-adgangskode til at være den samme som brugerens Windows-adgangskode. Denne funktion gennemtvingers ikke for drevadministratoren. Den gælder kun for drevbrugere. WPS -funktionaliteten kan bruges i virksomhedsmiljøer, hvor adgangskoder skal ændres med bestemte intervaller (f.eks. hver 90 dage). Hvis denne indstilling er aktiveret, opdateres alle brugeres SED-adgangskoder automatisk, når Windows-adgangskoderne ændres.

BEMÆRK: Når Windows password synchronization (WPS) er aktiveret, kan en brugers Self-Encrypting Drive-adgangskode ikke ændres. Windows-adgangskoden skal ændres for automatisk at kunne opdatere drevadgangskoden.

Husk sidste (Remember Last) Username (brugernavn)
Når denne indstilling er aktiveret, vises det senest indtastede brugernavn som standard i feltet **Brugernavn** (Username) på Pre-Windows-godkendelsesskærmen.

Brugernavn (Username) valg (Selection)
Når denne indstilling er aktiveret, kan brugere få vist alle drevbrugernavne i feltet **Brugernavn** (Username) på Pre-Windows-godkendelsesskærmen.

Kryptografisk (Cryptographic) sletning (Erase)
Denne indstilling kan bruges til at slette alle data på SED. Funktionen sletter ikke reelt dataene med de nøgler, der bruges til at kryptere data, og derfor bliver dataene ubrugelige. Det er ikke muligt at gendanne drevdata efter kryptografisk sletning. Derudover er SED-databeskyttelse deaktiveret, og drevet kan bruges til andre formål.

NOTER:
- Hvis der opstår fejl i funktionerne til SED-administration, skal du slukke computeren (ikke genstarte), og derefter tænde den igen.
- Hvis du vil have flere oplysninger om en bestemt fejlmeddelelse, skal du gå til wave.com/support/Dell.

Oplysninger om godkendelsesenhed (Authentication Device Information)

Vinduet Oplysninger om godkendelsesenhed (Authentication Device Information) i **Enhedshåndtering (Device Management)** indeholder oplysninger og status for alle tilsluttede godkendelsesenheder, f.eks. fingeraftrykslæser, traditionel eller contactless smartcardlæser) på systemet.

Teknisk support

Teknisk support til **Dell Data Protection | Adgang (Access)**-softwaren findes på http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP

Wave Systems Trusted Computing Group (TCG)-enabled Cryptographic Service Provider (CSP) er integreret i programmet **Dell Data Protection | Adgang (Access)** og kan anvendes, når der er brug for en CSP – enten via direkte opkald fra et program eller som valg fra en liste over installerede CSP'er. Hvis muligt, skal du vælge "Wave TCG-Enabled CSP" for at sikre, at TPM genererer -nøgler, og at nøglerne og de tilhørende adgangskoder administreres af **Dell Data Protection | Adgang (Access)**.

Wave Systems TCG-enabled CSP aktiverer programmer med funktioner på TCG-kompatible platforme direkte via MSCAPI. Dette er et TCG-forbedret MSCAPI CSP-modul, der giver asymmetrisk nøglefunktionalitet på TPM og udnytter den forbedrede sikkerhed, som TPM tilbyder, uden hensyntagen til leverandørspecifikke krav til leverandøren af Trusted Software Stack (TSS).

BEMÆRK: Hvis TPM-nøgler, som er genereret af Wave TCG-enabled CSP, kræver en adgangskode, og brugeren har oprettet en TPM masteradgangskode, genereres nøgleadgangskoderne helt vilkårligt og gemmes i TPM-adgangskodeboksen.