Startsidan för Dell dataskydd | Åtkomst

Startsidan för **Dell dataskydd | Åtkomst** är startpunkten när du vill använda funktionerna i programmet. Från det här fönstret når du följande alternativ:

System Access Wizard
Åtkomstalternativ
Självkrypterande enhet
Avancerade alternativ

Nere till höger i fönstret finns en länk med namnet **avancerat** som du kan klicka på för att komma åt avancerade alternativ.

Från Avancerade alternativ kan du klicka på länken **startsida** till höger i fönstrets nederkant när du vill gå tillbaka till startsidan.

System Access Wizard

System Access Wizard (guiden för systemåtkomst) startas automatiskt första gången programmet **Dell dataskydd | Åtkomst** startas. Den här guiden vägleder dig genom alla aspekter av systemets säkerhetskonfigurering, t.ex. hur (som exempelvis med lösenord eller fingeravtryck och lösenord) och när (i Windows, Pre-Windows eller båda) du loggar in i systemet. Om systemet har en självkrypterande enhet, kan du dessutom konfigurera den med hjälp av den här guiden.

Administratörsfunktioner

Användare som har Windows administratörsprivilegier på datorn har, till skillnad från standardanvändarna, behörighet att använda följande funktioner i **Dell dataåtkomst | Skydd**:

- Ställa in/ändra systemlösenord (Pre-Windows)
- Ställa in/ändra lösenord för hårddisken
- Ställa in/ändra administratörslösenord
- Ställa in/ändra TPM-ägarlösenordet
- Ställa in/ändra administratörslösenord för ControlVault
- Återställa systemet
- Arkivera och återställa autentiseringsuppgifter
- Ställa in/ändra administratörens PIN-kod till smartcard
- Rensa/återställa ett smartcard
- Aktivera/inaktivera Dell Säker inloggning i Windows
- Ange policy för Windows-inloggning
- Hantera självkrypterande enheter, bland annat:
    - Aktivera/inaktivera låsning av självkrypterande enhet
    - Aktivera/inaktivera WPS (Windows Password Synchronization)
    - Aktivera/inaktivera Single Sign On (SSO)
    - Genomföra en kryptografisk radering

Fjärrstyrd hantering

En organisation kan konfigurera en miljö där säkerhetsfunktionerna i programmet **Dell dataskydd | Åtkomst** hanteras centralt för många plattformar (dvs. fjärrstyrd hantering). I det här fallet kan Windows säkerhetsinfrastruktur, t.ex. Active Directory, användas för säker hantering av vissa funktioner i **Dell dataskydd | Åtkomst**.

När en dator hanteras via fjärrstyrning (dvs. "ägs" av fjärradministratören) kommer lokal administration av **Dell dataskydd | Åtkomst** att inaktiveras. Hanteringsfönstren i programmet går inte att nå lokalt. Hantering av följande funktioner kan göras via fjärrstyrning:

- Trusted Platform Module (TPM)
- ControlVault
- Pre-Windows-inloggning
- Återställa systemet
- BIOS-lösenord
- Policy för Windows-inloggning
- Självkrypterande enheter
- Registrering av fingeravtryck och smartcard

Om du vill veta mer om EMBASSY® Remote Administration Server (ERAS) för fjärrstyrd hantering från Wave Systems kontaktar du Dells säljrepresentant eller går till dell.com.

Åtkomstalternativ

Du kan ställa in hur du får åtkomst till systemet i fönstret Åtkomstalternativ.

Om du har gjort inställningar för **Dell dataskydd | Åtkomst** visas dessa på startsidan tillsammans med tillgängliga alternativ (t.ex. ändra lösenord för Pre-Windows-inloggning). Alternativen som visas är genvägar, som du kan klicka på för att öppna ett fönster där du kan genomföra en viss aktivitet (t.ex. ändra lösenordet för Pre-Windows-start eller registrera ett nytt fingeravtryck).

Allmänt
Först kan du ange när du vill logga in (Windows, Pre-Windows eller båda) och hur (t.ex. fingeravtryck och lösenord). Du kan välja ett eller två alternativ för inloggningen, dvs. olika kombinationer av fingeravtryck, smartcard och lösenord. Alternativen i listan baseras på den policy för inloggning som tillämpas i miljön där du arbetar och vilka metoder som stöds på plattformen.

Fingeravtryck
Om datorn har en fingeravtrycksläsare kan du registrera eller uppdatera fingeravtryck som du sedan kan använda för att logga in i systemet. När fingeravtrycken har registrerats, kan du svepa med fingret eller fingrarna som du har registrerat över fingeravtrycksläsaren för att få åtkomst till systemet i Windows, Pre-Windows eller bådadera (beroende på vilka inställningar du har valt i Allmänna åtkomstalternativ). Gå till Registrera fingeravtryck för användare om du vill veta mer.

Pre-Windows-inloggning
Om du har angett att användare måste logga in Pre-Windows måste du ställa in ett systemlösenord (kallas ibland Pre-Windows-lösenord) för att få åtkomst till datorn innan Windows startats. När lösenordet är inställt kan du som är administratör ändra lösenordet när du vill.

Du kan också inaktivera Pre-Windows-inloggning från den här skärmen. Det gör du genom att ange det aktuella systemlösenordet, bekräfta att lösenordet är korrekt och sedan klicka på knappen **Inaktivera**.

Smartcard
Om du har angett att användare måste använda ett smartcard för att logga in, måste du registrera ett eller flera smartcard (traditionella eller en nyare modell som inte kräver direktkontakt). Klicka på länken **Registrera ett nytt smartcard** om du vill starta guiden för registrering av smartcard. Med registrering menas att göra inställningar för ditt smartcard så att det kan användas för inloggning.

När du har registrerat ett smartcard kan du ändra eller ställa in en PIN-kod för kortet genom att använda länken **Ändra eller ställa in PIN-kod för smartcard**.

Pre-Windows-inloggning

När Pre-Windows-inloggning konfigurerats måste du autentisera dig (via lösenord, fingeravtryck eller smartcard) när strömmen till systemet slås på, innan Windows läses in. Funktionen för Pre-Windows-inloggning ger systemet en extra säkerhetsnivå som hindrar obehöriga användare från att skada Windows och komma åt datorn (om den t.ex. har stulits).

Från fönstret Pre-Windows-inloggning kan administratörer göra inställningar för Pre-Windows-inloggning, eller skapa och ändra ett Pre-Windows-lösenord (systemlösenord). Om det redan finns ett sådant lösenord kan du inaktivera Pre-Windows-inloggning från det här fönstret. Om du väljer att konfigurera Pre-Windows-inloggning startas en guide där du kan utföra följande:

- Systemlösenord: Ställa in ett systemlösenord (kallas också Pre-Windows-lösenord) för åtkomst innan Windows lästs in. Detta lösenord används också som en säkerhetskopia om en användare har ytterligare autentiseringsfaktorer (t.ex. för att få åtkomst till systemet om det blir fel på en fingeravtryckssensor).
- Fingeravtryck eller smartcard: Ställa in fingeravtryck eller smartcard för användning med Pre-Windows-inloggning, och ange om denna autentiseringsfaktor ska användas istället för, eller som tillägg till, Pre-Windows-lösenordet.
- Single Sign On: Som standard kommer din Pre-Windows-autentisering (lösenord, fingeravtryck eller smartcard) att användas för automatisk inloggning också i Windows (detta kallas "Single Sign On"). Du inaktiverar den här funktionen genom att välja kryssrutan "Jag vill logga in igen när Windows startas".
- Om ett BIOS-lösenord för hårddisken har ställts in som tillägg till ett Pre-Windows-lösenord, har du också möjlighet att ändra eller inaktivera lösenordet för hårddisken.

Obs! Alla fingeravtrycksläsare är inte aktiverade för användning med Pre-Windows-inloggning. Om läsaren inte är kompatibel kan du bara registrera fingeravtryck för Windows-inloggning. Du kan ta reda på om en viss fingeravtrycksläsare är kompatibel genom att kontakta systemadministratören eller kontrollera listan över hanterade fingeravtrycksläsare som finns på support.dell.com.

Inaktivera Pre-Windows-inloggning
Du kan också inaktivera Pre-Windows-inloggning från den här skärmen. Det gör du genom att ange det aktuella Pre-Windows- lösenordet (systemlösenordet), kontrollera att du har skrivit rätt lösenord och sedan klicka på knappen **Inaktivera**. Observera att alla registrerade fingeravtryck eller smartcard förblir registrerade när du inaktiverar Pre-Windows-inloggning.

Registrera/ta bort fingeravtryck

Användare kan registrera eller uppdatera fingeravtryck som kan användas för autentisering i systemet, antingen vid Pre-Windows- eller Windows-inloggning. På fliken Fingeravtryck visas bilder av en hand där de fingrar som registrerats är markerade (om registreringen är klar). Om du klickar på länken **Registrera ett nytt finger** startas guiden Fingerprint Enrollment, som vägleder dig genom registreringsprocessen. Med "registrering" menas att spara ett fingeravtryck som kan användas för inloggning. Det måste finnas en giltig fingeravtryckskläsare installerad och konfigurerad för att du ska kunna registrera fingeravtryck.

Obs! Alla fingeravtryckskläsare fungerar inte med Pre-Windows-inloggning. Ett felmeddelande visas om du försöker registrera dig för Pre-Windows-inloggning med en inkompatibel läsare. Du kan ta reda på om enheten är kompatibel genom att kontakta systemadministratören eller kontrollera listan över hanterade fingeravtryckskläsare som finns på support.dell.com.

När du registrerar fingeravtryck uppmanas du att ange Windows-lösenordet som verifiering på din identitet. Om systemets policy kräver det, visas även en uppmaning om att ange Pre-Windows-lösenordet (Systemlösenordet). Du kan behöva Pre-Windows-lösenordet för att få åtkomst till systemet om det inträffar ett fel med fingeravtryckskläsaren.

Obs!

- Vi rekommenderar att du registrerar minst två fingeravtryck under registreringsprocessen.
- Du måste se till att fingeravtrycken är korrekt registrerade innan du aktiverar funktionerna för fingeravtrycksautentisering.
- Om du byter fingeravtryckskläsare i systemet måste du registrera om fingeravtrycken med den nya läsaren. Vi rekommenderar inte att man växlar mellan två olika fingeravtryckskläsare.
- Om det visas upprepade meddelanden om att "Sensorn förlorade fokus" vid registrering av fingeravtryck kan det betyda att datorn inte kan identifiera fingeravtryckskläsaren. Om du har en extern fingeravtryckskläsare kan du prova med att koppla bort och återansluta fingeravtryckskläsaren. Det räcker ofta för att lösa problemet.

Rensa registrerade fingeravtryck
Du kan ta bort registrerade fingeravtryck genom att klicka på länken **Ta bort fingeravtryck** eller genom att klicka på (så att det avmarkeras) ett registrerat finger i guiden Fingerprint Enrollment.

En administratör kan ta bort en viss användare som har registrerat fingeravtryck för Pre-Windows-autentisering genom att avmarkera alla fingeravtryck som registrerats för den användaren.

Obs! Om det visas felmeddelanden medan du registrerar fingeravtryck kan du gå till wave.com/support/Dell för mer information.

Registrera smartcard

I **Dell dataskydd | Åtkomst** kan du välja mellan traditionellt (för anslutning) eller contactless (ansluts ej) smartcard för inloggning på Windows-kontot eller för Pre-Windows-autentisering. Om du klickar på länken **Registrera ett nytt smartcard** startas guiden för registrering av smartcard, som vägleder dig genom registreringsprocessen. Med "registrering" menas att göra inställningar för ditt smartcard så att det kan användas vid inloggning.

Det måste finnas en giltig enhet för smartcardautentisering installerad och konfigurerad för att du ska kunna registrera.

Obs! Om du vill ta reda på om en viss enhet är kompatibel kontaktar du systemadministratören eller kontrollerar listan över hanterade smartcard på support.dell.com.

Registrering
När du registrerar ett smartcard uppmanas du att ange Windows-lösenordet som verifiering på din identitet. Om systemets policy kräver det, visas även en uppmaning om att ange Pre-Windows-lösenordet (Systemlösenordet). Du kan behöva Pre-Windows-lösenordet för att få åtkomst till systemet om det blir fel på smartcardläsaren.

Under registrering uppmanas du att ange PIN-koden för ditt smartcard, om du har en sådan. Om du måste ange en PIN-kod enligt systemets policy men ingen har ställts in, visas en ruta där du kan skapa en kod.

Obs!

- När en användare registrerats för smartcardanvändning i Pre-Windows går det inte att ta bort honom eller henne.
- Standardanvändare kan ändra sin PIN-kod för ett smartcard, och administratören kan ändra både administratörens PIN -kod och användarens PIN-kod.
- Administratören kan också återställa ett smartcard. Ett smartcard som återställts kan inte användas för autentisering vid Windows-inloggning eller Pre-Windows förrän det registrerats på nytt.

Obs! För autentisering av TPM-certifikat kan administratörer registrera TPM-certifikat via registreringsprocessen för smartcard i Microsoft Windows. Administratörer måste välja "Wave TCG-Enabled CSP" som kryptografiprovider istället för en smartcard-CSP för att funktionen ska vara kompatibel med det här programmet. Dessutom måste Dell Säker inloggning vara aktiverat med rätt autentiseringstyppolicy för klienten.

Obs! Om det visas ett felmeddelande som anger att Smartcard-tjänsten inte är igång, kan du starta/starta om tjänsten så här:

- Gå till fönstret Administrationsverktyg från Kontrollpanelen, välj Tjänster, högerklicka sedan på Smartcard och välj Starta eller Starta om.
- Om du vill veta mer om ett visst felmeddelande kan du gå till wave.com/support/Dell.

Självkrypterande enhet

Med **Dell dataskydd | Åtkomst** hanterar du de maskinvarubaserade säkerhetsfunktionerna för sådana självkrypterande enheter, som har funktioner för datakryptering inbyggda i enhetens maskinvara. Funktionen säkerställer att endast behöriga användare kan få åtkomst till krypterade data (när enhetslåsning är aktiverat).

Fönstret Självkrypterande enhet öppnas när du klickar på fliken **Självkrypterande enhet** i nederkanten. Fliken visas bara när det finns en eller flera självkrypterande enheter i systemet.

Klicka på länken **Installera** när du vill starta Installationsguiden för självkrypterande enheter. Med hjälp av den här guiden kan du skapa ett lösenord för enhetens administratör, säkerhetskopiera lösenordet och tillämpa inställningarna för enhetskryptering. Det är bara systemadministratörer som kan köra Installationsguiden för självkrypterande enheter.

Viktigt! När enheten är konfigurerad kommer funktionerna för dataskydd och enhetslåsning att vara "aktiverade". En låst enhet har följande beteende:

- Enheten går till *låst* läge när strömmen till enheten slås på.
- Det går inte att starta enheten om inte användaren loggar in med korrekt användarnamn och lösenord (eller fingeravtryck) på Pre-Windows-skärmen. Innan enhetslåsning aktiverats är data på enheten tillgängliga för alla användare på datorn.
- Enheten är skyddad även om den ansluts till en annan dator som sekundär enhet – autentisering krävs för att få åtkomst till enhetens data.

När enheten har konfigurerats, visas fönstret Självkrypterande enhet med enheten (eller enheterna) samt en länk för användarna där de kan ändra sina lösenord till enheten. Om du är enhetsadministratör kan du också lägga till eller ta bort användare för enheten i det här fönstret. Om det var en extern enhet som du konfigurerade, visas den i det här fönstret så att du kan låsa upp den.

OBS: En sekundär (extern) enhet måste kunna stängas av fristående från datorn för att kunna låsas.

Enhetens administratör hanterar enhetsinställningarna i **Avancerat>Enheter**. Se Enhetshantering – Självkrypterande enheter för mer information.

Installera enheten

Installationsguiden för självkrypterande enheter vägleder dig genom konfigureringen av enheten eller enheterna. Följande begrepp är viktiga att känna till när du går igenom den här processen.

Enhetens administratör
Den första användare med systemadministratörsbehörighet som konfigurerar enhetsåtkomsten (och ställer in lösenordet för enhetsadministratören) blir också enhetens administratör. Detta är den enda användare som har behörighet att göra ändringar i enhetsåtkomsten. Det är viktigt att se till att den första användaren som ställs in som enhetens administratör är rätt användare. Innan du kan fortsätta med det här steget måste du därför markera kryssrutan "Jag har förstått".

Enhetens administratörslösenord
I guiden visas uppmaningar om att du måste skapa ett administratörslösenord för enheten och ange lösenordet en gång till som bekräftelse. Du måste ange ditt Windows-lösenord för att bekräfta din identitet innan du kan skapa ett administratörslösenord för enheten. Den aktuella Windows-användaren måste ha administratörsbehörighet för att kunna skapa det här lösenordet.

Säkerhetskopiera autentiseringsuppgifter för enhet
Ange en plats eller klicka på **Bläddra** och välj en plats där du vill spara en säkerhetskopia av dina autentiseringsuppgifter som enhetens administratör.

VIKTIGT**!**

- Vi rekommenderar starkt att du säkerhetskopierar autentiseringsuppgifterna, samt att du säkerhetskopierar dem till en annan enhet än den primära hårddisken (t.ex. ett flyttbart media). Annars riskerar du att inte få åtkomst till säkerhetskopian om du skulle förlora åtkomsten till den ordinarie hårddisken.
- När du har slutfört enhetskonfigureringen måste allaanvändare ange rätt användarnamn och lösenord (eller fingeravtryck) innan Windows läses in för att få åtkomst till systemet nästa gång strömmen slås på.

Lägga till enhetsanvändare
Enhetens administratör kan lägga till andra giltiga Windows-användare som användare på enheten. När användare läggs till på enheten kan administratören begära att användaren återställer sitt lösenord vid första inloggningen. Användaren måste då återställa sitt lösenord vid autentisering på Pre-Windows-skärmen innan enheten låses upp.

Avancerade inställningar

- *Single Sign On* - Som standard kommer ditt lösenord till den självkrypterande enheten, som du anger som autentisering för enheten innan Windows läses in, att användas för automatisk inloggning även i Windows (detta kallas samlad inloggning, dvs. "Single Sign On"). Du kan inaktivera den här funktionen genom att välja kryssrutan "Jag vill logga in igen när Windows startas" när du konfigurerar enhetsinställningarna.
- *Logga in med fingeravtryck* – På plattformar där funktionen fungerar kan du ange att du vill autentisera dig för den självkrypterande enheten med hjälp av fingeravtryck istället för med lösenord.
- *Support för standby/vänteläge (S3)* (om plattformen hanterar funktionen) - När funktionen är aktiverad kan den självkrypterande enheten försättas i standby/vänteläge på ett säkert sätt (kallas även S3-läge) och kräva Pre-Windows-autentisering vid återgång från standby/vänteläge.

Obs!

- När stöd för S3 är aktiverat måste lösenorden för krypterade enheter utformas i enlighet med eventuella begränsningar för lösenord i BIOS. Kontakta maskinvarutillverkaren om du vill veta mer om specifika BIOS-lösenordsbegränsningar som kan finnas för systemet.
- S3-läget hanteras inte av alla självkrypterande enheter. Under enhetskonfigureringen får du ett meddelande om enheten har stöd för standby/vänteläge eller inte. För enheter som inte har stöd för det här läget omvandlas automatiskt en begäran från Windows om att gå till S3-läge till viloläge, om viloläget är aktiverat (vi rekommenderar starkt att du aktiverar viloläge på datorn).
- Första gången du loggar in efter att alternativet Single Sign On (SSO) har ställts in kommer processen att göra en paus vid Windows inloggningsskärm. Du måste ange din typ av Windows-autentisering, som lagras säkert för framtida inloggningsförsök till Windows. Nästa gång systemet startas kommer SSO att automatiskt logga in dig i Windows. Samma process är också nödvändig när en användares autentiseringsuppgifter för Windows (lösenord, fingeravtryck, PIN-kod till smartcard) ändras. Om datorn finns i en domän, och domänen har en policy som kräver att tangenterna Ctrl+Alt+Del måste tryckas ned för Windows-inloggning, kommer denna policy att upprätthållas.

VARNING! Om du avinstallerar programmet **Dell dataskydd | Åtkomst** måste du först inaktivera dataskyddet för självkrypterande enheter och låsa upp enheten.

Användarfunktioner för självkrypterande enhet

Administratörer för självkrypterande enheter genomför allt underhåll för enhetens säkerhet och användare. Enhetsanvändare som inte är administratörer för enheten kan bara utföra följande uppgifter:

- Ändra sina egna enhetslösenord
- Låsa upp en enhet

Dessa aktiviteter kan nås från fliken **Självkrypterande enhet** i **Dell dataskydd | Åtkomst**.

Byt lösenord
Detta gör att registrerade användare kan skapa nya lösenord för enhetsautentisering. Du måste ange ditt nuvarande lösenord för en självkrypterande enhet innan enhetslösenordet ställs in på det nya värdet.

Obs!

- Programmet tillämpar Windows regler för lösenordets längd och komplexitet, om de har aktiverats. Om Windows lösenordspolicy inte har aktiverats är den maximala längden för ett lösenord för en självkrypterande enhet 32 tecken. Observera att maximala längden är 127 tecken om S3 (Vänteläge/standby) inte är aktiverat.
- En användares lösenord för en självkrypterande enhet skiljer sig från Windows-lösenordet. När en användares Windows-lösenord ändras eller återställs påverkar det inte användarens enhetslösenord, såvida inte WPS-funktionen för synkronisering med Windows-lösenordet har aktiverats. Mer information finns i Enheter: Självkrypterande enheter.
- På vissa icke-engelska tangentbord finns en extra uppsättning tecken som inte kan användas i lösenordet för en självkrypterande enhet. Om Windows-lösenordet innehåller något av de otillåtna tecknen och om du har aktiverat Windows-lösenordssynkronisering kommer synkroniseringen att misslyckas och ett felmeddelande visas.

Låsa upp enhet
Med alternativet Låsa upp enhet kan en registrerad enhetsanvändare låsa upp en låst enhet. Om enhetslåsning har aktiverats går enheten över i låst läge när strömmen till datorn slås av. När strömmen till systemet slås på igen, måste du autentisera dig för enheten genom att ange lösenordet på Pre-Windows-skärmen för autentisering.

Obs!

- Systemet kan hindras från att gå över i strömsparläge (som vänteläge/standby eller viloläge) om flera användarkonton för en självkrypterande enhet är aktiva samtidigt på datorn.
- På skärmen för Pre-Windows-autentisering byts "Användare 1", "Användare 2", osv. ut mot namnen på enhetsanvändaren i versioner av programmet som har lokaliserats till följande språk: kinesiska, japanska, koreanska och ryska.

Avancerade alternativ

Med Avancerade alternativ i **Dell dataskydd | Åtkomst** kan du aktivera en användare med administratörsprivilegier så att han eller hon får möjlighet att hantera följande inställningar i programmet:

Underhåll
Lösenord
Enheter

Obs! Det är bara användare med administratörsprivilegier som kan göra ändringar i Avancerade alternativ. Standardanvändare kan visa inställningarna men inte göra några ändringar.

Underhåll

I fönstret Underhåll kan administratörer konfigurera inställningar för Windows-inloggning, återställa ett system som en förberedelse på att använda det för ett annat syfte, eller arkivera och återställa användares autentiseringsuppgifter som lagrats på systemets säkerhetsmaskinvara. Mer information finns i följande avsnitt:

Åtkomstinställningar
Återställa systemet
Arkivera och återställa autentiseringsuppgifter

Åtkomstinställningar

I fönstret Åtkomstinställningar kan administratörer ange inställningar för Windows-inloggning för alla användare i systemet.

Aktivera Dell Säker inloggning
Du kan ersätta Windows standardskärm (med Ctrl-Alt-Delete) och använda andra autentiseringsmetoder istället för (eller som komplement till) Windows-lösenordet för att ge åtkomst till Windows. Du kan välja att lägga till fingeravtryck som en extra autentiseringsfaktor för att få ännu starkare skydd för Windows-inloggningen. Det finns också andra autentiseringsfaktorer, som exempelvis ett smartcard eller ett TPM-certifikat, som kan användas för Windows-inloggning.

Obs!

- Att aktivera Dell Säker inloggning påverkar alla användare i systemet.
- Vi rekommenderar att alternativet aktiveras EFTER att användarna har registrerat fingeravtryck eller smartcard.
- Första gången du loggar in efter att alternativet har ställts in uppmanas du att autentisera dig i Windows enligt standardpolicyn, men från och med nästa systemstart måste du använda den nya autentiseringsfaktorn (eller -faktorerna).

Inaktivera Dell Säker inloggning
Med det här alternativet inaktiveras alla funktioner i **Dell dataskydd | Åtkomst** för inloggning i Windows. När du väljer det här alternativet börjar standardpolicyn för inloggning i Windows åter att gälla.

Obs!

- Om det inträffar ett fel när du försöker använda säker inloggning i Windows, ska du inaktivera alternativet Dell Säker inloggning och sedan aktivera det igen.
- Om du vill veta mer om ett visst felmeddelande kan du gå till wave.com/support/Dell.

Återställa systemet

Funktionen Återställ systemet används för att rensa alla användardata från all säkerhetsmaskinvara på plattformen. Det kan t.ex. användas när en dator ska återanvändas för ett annat syfte. Med det här alternativet rensar du alla lösenord i systemet, förutom användarlösenorden till Windows, såväl som alla data på maskinvaruenheterna (t.ex. ControlVault, TPM och fingeravtryckläsare). För självkrypterande enheter kommer den här funktionen också att inaktivera dataskyddet så att enhetsdata blir tillgängliga.

Du måste bekräfta att du vill återställa systemet och sedan klickar du på **Nästa**. När du återställer systemet måste du ange lösenordet för varje säkerhetsenhet, om sådana finns:

- TPM-ägare
- ControlVault-administratör
- BIOS-administratör
- BIOS-system (Pre-Windows)
- Hårddisk (BIOS)
- Administratör för självkrypterande enhet

Obs! För självkrypterande enheter krävs endast administratörslösenordet till enheten, inte samtliga enhetsanvändares lösenord.

Viktigt! Det enda sättet att återskapa data som rensas bort när du återställer ett system är att återställa från ett sparat arkiv. Om du inte har ett arkiv kan data inte återskapas. För en självkrypterande enhet tas endast konfigureringsdata bort. Inga personliga data tas bort från enheten.

Arkivera och återställa autentiseringsuppgifter

Funktionerna för att arkivera och återställa autentiseringsuppgifter används för att säkerhetskopiera och återställa alla användarens autentiseringsuppgifter (inloggnings- och krypteringsinformation) som lagrats i ControlVault och i Trusted Platform Module (TPM). Det är viktigt att ha en säkerhetskopia av denna information om systemet måste återskapas på en dator eller om du behöver återställa data efter ett fel på maskinvaran. Om detta inträffar är det enkelt att återställa samtliga autentiseringsuppgifter på den nya datorn från en sparad arkivfil.

Du kan välja mellan att arkivera eller återställa autentiseringsuppgifter för en enstaka användare eller för alla användare i systemet.

Användarens autentiseringsuppgifter utgörs av data som används i Pre-Windows-miljö, t.ex. registrerade fingeravtryck och smartcarddata, samt nycklar som lagrats i TPM. TPM skapar nycklar vid begäran från säkra program – om du t.ex. genererar ett digitalt certifikat skapas nycklar i TPM.

Obs! Om du vill veta om dina TPM-nycklar kan arkiveras av **Dell dataskydd | Åtkomst** går du till dokumentationen för det skyddade programmet. Program som använder ”Wave TCG-Enabled CSP” för att generera nycklar har vanligen det nödvändiga stödet.

Arkivera autentiseringsuppgifter
Du måste göra följande för att kunna arkivera autentiseringsuppgifter:

- Ange om du arkiverar autentiseringsuppgifter för egen räkning eller för alla användare i systemet.
- Autentisera dig för maskinvaran som används i säkerhetsrutinerna genom att ange systemlösenordet (Pre-Windows), administratörslösenordet för ControlVault samt TPM-ägarlösenordet.
- Skapa ett lösenord för säkerhetskopian av autentiseringsuppgifterna.
- Välja en arkiveringsplats genom att använda knappen **Bläddra**. Arkiveringsplatsen måste vara ett flyttbart media, t.ex ett USB-minne eller en nätverksenhet, för att skydda innehållet vid maskinvarukrascher.

Viktigt:
- Anteckna arkiveringsplatsen eftersom användaren måste ha denna information för att kunna återställa autentiseringsuppgifterna.
- Anteckna lösenordet till säkerhetskopian med autentiseringsuppgifterna så att data kan återställas vid behov. Det är viktigt eftersom detta lösenord inte kan återställas.
- Om du inte känner till TPM-ägarlösenordet kan du kontakta systemadministratören eller läsa datorns TPM-installationsinstruktioner.

Återställa autentiseringsuppgifter
Du måste göra följande för att kunna återställa autentiseringsuppgifter:

- Ange om du återställer autentiseringsuppgifter för egen räkning eller för alla användare i systemet.
- Bläddra till arkiveringsplatsen och välja arkivfilen.
- Ange lösenordet till säkerhetskopian med autentiseringsuppgifterna som skapades när du konfigurerade arkivet.
- Autentisera dig för maskinvaran som används i säkerhetsrutinerna genom att ange systemlösenordet (Pre-Windows), administratörslösenordet för ControlVault samt TPM-ägarlösenordet.

Obs!

- Om det visas ett felmeddelande om att det inte gick att återställa autentiseringsuppgifterna och du redan har gjort flera försök att återställa, försöker du återställa en annan arkivfil. Om inte heller detta lyckas, skapar du ett annat autentiseringsarkiv och gör ett försök att återställa från det nya arkivet.
- Om du får ett felmeddelande om att TPM-nycklarna inte kunde återställas, skapar du ett autentiseringsarkiv och rensar sedan TPM i BIOS. Om du vill rensa TPM ska du starta om datorn, trycka på tangenten **F2** när den startar upp igen så att du kommer till BIOS - inställningarna och sedan gå till Säkerhet>TPM-säkerhet. Gör om inställningarna för TPM-ägare och gör ett nytt försök att återställa autentiseringsuppgifterna.
- Om du vill veta mer om ett visst felmeddelande kan du gå till wave.com/support/Dell.

Lösenordshantering

I fönstret Lösenordshantering kan en administratör skapa eller ändra samtliga säkerhetslösenord i systemet:

- System (kallas också Pre-Windows)*
- Administratör*
- Hårddisk*
- ControlVault
- TPM-ägare
- TPM-huvudlösenord
- Lösenordsvalv i TPM
- Självkrypterande enhet

Obs!

- Det är bara de lösenord som är tillämpliga i den aktuella plattformskonfigurationen som visas. Fönstrets innehåll varierar alltså beroende på systemets konfiguration och status.
- De lösenord som är märkta med * här ovan är BIOS-lösenord vilka också kan ändras via systemets BIOS.
- Lösenord på BIOS-nivå kan inte skapas eller ändras om BIOS-administratören har nekat lösenordsändringar.
- Om du klickar på länken **installera** för en självkrypterande enhet startas guiden Self-Encrypting Drive Setup. Om du klickar på **hantera** kan en användare ändra ett eller flera lösenord för självkrypterande enheter.
- Om du klickar på länken **hantera** för lösenordsvalvet i TPM visas ett fönster där du kan visa eller ändra lösenorden som skyddar dina TPM-nycklar. När en TPM-nyckel som kräver ett lösenord skapas, genereras lösenordet slumpmässigt och placeras i valvet. Du kan inte hantera lösenordsvalvet i TPM förrän du har skapat ett TPM-huvudlösenord.

Windows komplexitetsregler för lösenord

Dell dataskydd | Åtkomst säkerställer att följande lösenord utformas enligt Windows komplixitetsregler för datorns lösenord:

- TPM-ägarlösenord

När du vill bestämma policy för komplexitet för Windows-lösenord följer du dessa steg:

1. Öppna Kontrollpanelen.
2. Dubbelklicka på Administrationsverktyg.
3. Dubbelklicka på Lokala säkerhetsprinciper.
4. Utöka Kontoprinciper och välj Lösenordsprincip

Enheter

Med hjälp av fönstret Enheter kan administratörer hantera alla säkerhetsenheter som är installerade i systemet. För varje enhet kan du visa status och ytterligare detaljer, som exempelvis version för fast programvara. Klicka på **visa** när du vill visa informationen om en enhet och **dölj** när du vill dölja detaljerna i ett avsnitt. Följande enheter kan hanteras, beroende på vilka plattformen innehåller:

Trusted Platform Module (TPM)
ControlVault®
Självkrypterande enheter
Information om enhet för autentisering

Trusted Platform Module (TPM)

TPM-säkerhetskretsen måste vara aktiverad och ägarskapet för TPM måste vara upprättat för att du ska kunna använda de avancerade säkerhetsfunktionerna som är tillgängliga i **Dell dataskydd | Åtkomst** och TPM.

Fönstret Trusted Platform Module i **Enhetshantering** visas bara när en TPM kan identifieras i systemet.

TPM-administration

Med hjälp av de här funktionerna kan systemadministratören hanteraTPM.

Status

Visar statusen *aktiv* eller *inaktiv* för TPM. Statusen "Aktiv" betyder att TPM har aktiverats i BIOS och att funktionen kan börja konfigureras (dvs. ägarskap kan ställas in). TPM kan inte hanteras och säkerhetsfunktionerna kan inte öppnas om inte TPM är aktivt (aktiverat).

Om TPM identifieras i systemet men inte är aktivt (aktiverat) kan du aktivera funktionen genom att klicka på länken **aktivera** i det här fönstret, utan att behöva gå till systemets BIOS. När du har aktiverat TPM med den här funktionen måste datorn startas om. Under omstarten kan det visas ett meddelande där du får bekräfta att du accepterar ändringarna.

Obs! Möjligheten att aktivera TPM från det här programmet stöds inte på alla plattformar. Om alternativet inte stöds, måste du aktivera funktionen i systemets BIOS. Det gör du genom att starta om systemet och trycka på tangenten **F2** innan Windows läses in så att du kommer till BIOS-inställningarna. Sedan går du till Säkerhet>TPM-säkerhet och aktiverar TPM.

Du kan också *inaktivera* TPM härifrån genom att klicka på länken **inaktivera**. (Om du inaktiverar TPM blir funktionen inte tillgänglig för de avancerade säkerhetsfunktionerna.) Vid inaktiveringen ändras dock inte några TPM-inställningar, och ingen information eller nycklar som lagrats i TPM tas bort eller ändras.

Ägd

Visar statusen för ägarskap (t.ex. "ägd") och du kan skapa eller ändra TPM-ägare. Ägarskapet för TPM måste upprättas för att säkerhetsfunktionerna i TPM ska vara tillgängliga. TPM måste aktiveras innan ägarskapet kan upprättas.

I proceduren för att upprätta ett ägarskap ingår att användaren (med administratörsprivilegier) skapar ett TPM-ägarlösenord. När detta lösenord har definierats utses en ägare och TPM är klart att användas.

Obs! TPM-ägarlösenord måste utformas i enlighet med Windows komplexitetsregler för lösenord i systemet.

Viktigt! Det är viktigt att du inte förlorar eller glömmer TPM-ägarlösenordet, eftersom det krävs för att få åtkomst till avancerade säkerhetsfunktioner för TPM i **Dell dataskydd | Åtkomst**.

Låst

Visar statusen *låst* eller *olåst* för TPM. "Låsning" är en säkerhetsfunktion i TPM; TPM går till låst läge efter det angivna antalet felaktiga TPM-ägarlösenord. TPM-ägaren kan låsa upp TPM härifrån, men TPM-ägarlösenordet måste anges.

Obs!

- Om det visas ett felmeddelande om att ägarskapet för TPM inte kunde upprättas, rensar du TPM i systemets BIOS och gör ett nytt försök. Du rensar TPM genom att starta om

datorn, trycka på tangenten **F2** under starten så att du kommer till BIOS-inställningarna och sedan gå till Säkerhet>TPM-säkerhet.

- Om det visas ett felmeddelande som anger att TPM-ägarlösenordet inte kunde ändras, arkiverar du TPM-data (arkivera autentiseringsuppgifter), rensar TPM i BIOS, återupprättar ägarskapet för TPM och återställer TPM-data (återställer autentiseringsuppgifter).
- Om du vill veta mer om ett visst felmeddelande kan du gå till wave.com/support/Dell.

Dell ControlVault®

Dell ControlVault® (CV) är ett säkert maskinvarubaserat lager för användarnas autentiseringsuppgifter som används vid Pre-Windows-inloggningar (det kan t.ex. gälla användarlösenord eller registrerade fingeravtrycksdata). Fönstret ControlVault i **Enhetshantering** visas bara om en ControlVault kan identifieras i systemet.

ControlVault-administration

Med de här funktionerna kan systemadministratören hantera systemets ControlVault.

Status
Visar statusen *aktiv* eller *inaktiv* för ControlVault-enheten. Statusen "inaktiv" betyder att ControlVault-enheten inte är tillgänglig för lagring av data i systemet. Gå till Dells systemdokumentation och kontrollera om systemet innehåller en ControlVault.

Lösenord
Anger om administratörslösenordet för ControlVault har ställts in, och ger möjlighet att ställa in ett lösenord eller ändra lösenordet (om det redan är inställt). Det är bara systemadministratörer som kan ställa in eller ändra det här lösenordet. Ett administratörslösenord för ControlVault måste ställas in för att du ska kunna:

- Genomföra en arkivering eller återställning av autentiseringsuppgifter.
- Rensa användardata (för alla användare).

Obs! Om en användare gör ett försök att arkivera eller återställa innan administratörslösenordet för ControlVault har ställts in, får användaren en uppmaning om att skapa ett sådant lösenord (om användaren är administratör).

Registrerade användare
Anger om några användare har registrerat autentiseringsuppgifter för inloggning (t.ex. lösenord, fingeravtryck eller smartcarddata) som finns lagrade i ControlVault.

Rensa användardata
Data i ControlVault kan ibland behöva rensas. Det kan t.ex. hända om det inträffar problem när användare försöker använda eller registrera autentiseringsuppgifter för Pre-Windows-inloggning. Alla data som lagrats i ControlVault kan rensas, för en enstaka användare eller för alla användare, från det här fönstret.

Administratörslösenordet för ControlVault måste anges för att du ska kunna rensa alla användardata på plattformen. Du måste också ange systemlösenordet (Pre-Windows) om autentiseringsuppgifter för Pre-Windows-inloggning registrerats. När du rensar alla användardata, kommer administratörslösenordet för ControlVault och systemlösenordet att återställas. Notera att det här är det enda sättet att rensa administratörslösenordet för ControlVault.

Obs! När du har rensat alla användardata visas en uppmaning om att starta om datorn. Det är viktigt att du startar om för att systemet ska fungera som avsett.

Administratörslösenordet för ControlVault behöver inte ställas in för att rensa en enstaka användares autentiseringsuppgifter. När du klickar på **rensa användardata** visas ett meddelande om att välja användaren vars autentiseringsuppgifter för ControlVault du vill rensa. När du har valt en användare uppmanas du att ange systemlösenordet (gäller bara om autentiseringsuppgifter för Pre-Windows registrerats).

Obs!

- Om det visas ett felmeddelande som anger att administratörslösenordet för ControlVault inte kan skapas måste du arkivera dina autentiseringsuppgifter, rensa alla användardata från ControlVault, starta om datorn och försöka skapa lösenordet igen.
- Om det visas ett felmeddelande som anger att autentiseringsuppgifter för en enstaka användare inte kunde rensas från ControlVault, ska du arkivera dina autentiseringsuppgifter, prova med att rensa alla användardata och sedan försöka rensa data för den enstaka användaren igen.
- Om det visas ett felmeddelande som anger att autentiseringsuppgifter inte kunde rensas från ControlVault för alla användare, bör du överväga att genomföra en systemåterställning. **Viktigt!** Läs igenom hjälpavsnittet Återställa systemet innan du genomför en återställning eftersom det innebär att ALL säkerhetsinformation för användarna rensas bort.
- Om det visas ett felmeddelande som anger att ControlVault- och TPM-data inte kunde säkerhetskopieras, inaktiverar du TPM i systemets BIOS. Det görs genom att du startar om datorn och trycker på tangenten **F2** när den startar upp igen så att du kommer till BIOS-inställningarna. Sedan går du till Säkerhet>TPM-säkerhet. Därefter kan du återaktivera TPM och försöka arkivera ControlVault-data en gång till.
- Om du vill veta mer om ett visst felmeddelande kan du gå till wave.com/support/Dell.

Självkrypterande enheter: Avancerat

Med **Dell dataskydd | Åtkomst** kan du hantera de maskinvarubaserade säkerhetsfunktionerna för sådana självkrypterande enheter som har funktioner för datakryptering inbyggda i enhetens maskinvara. Hanteringsfunktionen säkerställer att endast auktoriserade användare kan få åtkomst till krypterade data när enhetslåsning är aktiverat.

Fönstret Självkrypterande enhet i **Enhetshantering** visas bara när det finns en eller flera självkrypterande enheter (SED) i systemet.

Viktigt! När enheten är konfigurerad kommer dataskyddet för den självkrypterande enheten och enhetslåsning att vara "aktiverade".

Enhetshantering
Med hjälp av dessa funktioner kan enhetens administratör hantera säkerhetsinställningarna. Ändringar i enhetens säkerhetsinställningar verkställs när strömmen till enheten har stängts av.

Dataskydd
Visar om statusen för dataskyddet för den självkrypterande enheten är *aktiverad* eller *inaktiverad*. Statusen "aktiverad" betyder att säkerhetsfunktionerna för enheten är konfigurerade, men användarna behöver inte ange autentiseringsuppgifter för enheten före inläsning av Windows förrän *enhetslåsning* har slagits på.

Härifrån kan du inaktivera dataskyddet för en självkrypterande enhet. När det är inaktiverat stängs alla avancerade säkerhetsfunktioner för den självkrypterande enheten av och enheten fungerar som en standardenhet. När du inaktiverar dataskyddet tas alla säkerhetsinställningar bort, inklusive autentiseringsuppgifter för enhetens administratör och enhetens användare. Funktionen innebär inte att några användardata på enheten ändras eller tas bort.

Låsning
Här visas statusen *aktiverad* eller *inaktiverad* för den självkrypterande enheten eller enheterna. Gå till avsnittet Självkrypterande enhet om du vill veta mer om hur en låst enhet fungerar.

Här kan du också tillfälligt inaktivera enhetslåsningen, vilket ibland kan vara nödvändigt. Det rekommenderas inte eftersom det inte krävs några autentiseringsuppgifter för att få åtkomst till enheten när enhetslåsningen är inaktiverad, vilket innebär att alla användare på plattformen kan få åtkomst till data på enheten. Ingasäkerhetsinställningar, inklusive autentiseringsuppgifterna för enhetens administratör och användare eller användardata på enheten, tas bort när du inaktiverar enhetslåsning.

VARNING! Om du avinstallerar programmet **Dell dataskydd | Åtkomst** måste du först inaktivera dataskyddet för självkrypterande enheter och låsa upp enheten.

Enhetens administratör

Visar vem som är administratör för enheten för närvarande. Enhetens administratör kan ändra vilken användare som är administratör härifrån. Den nya administratören måste vara en giltig Windows-användare i systemet och ha administratörsprivilegier. Det kan bara finnas en administratör för enheten i systemet.

Enhetsanvändare

Visar de registrerade enhetsanvändarna, samt hur många användare som är registrerade just nu. Hur många användare som stöds beror på den självkrypterande enheten (för närvarande 4 användare för Seagate-enheter och 24 för Samsung-enheter).

Windows Password Sync

WPS-funktionen (Windows Password Synchronization) ställer automatiskt in användarnas lösenord till en självkrypterande enhet till samma lösenord som de använder i Windows. Den här funktionen tillämpas inte för enhetens administratör, utan används bara för enhetsanvändarna. WPS-funktionerna kan användas i företagsmiljöer där lösenord måste ändras med vissa tidsintervall (t.ex. var 90:e dag). När det här alternativet är aktiverat kommer alla användares lösenord till självkrypterande enheter att uppdateras automatiskt när de ändrar sina Windows-lösenord.

Obs! När WPS-funktionen är aktiverad kan användarens lösenord till en självkrypterande enhet inte ändras. Respektive Windows-lösenord måste ändras först, varpå enhetslösenordet uppdateras automatiskt.

Kom ihåg senaste användarnamnet

När det här alternativet är aktiverat kommer det senaste användarnamn som angetts att visas som standard i fältet **Användarnamn** på Pre-Windows-skärmen för autentisering.

Val av användarnamn

När det här alternativet är aktiverat kan användare visa alla användarnamn för enheten i fältet **Användarnamn** på Pre-Windows-skärmen för autentisering.

Kryptografisk radering

Med det här alternativet kan du "radera" alla data på den självkrypterande enheten. I praktiken tas dock data inte bort, utan bara nycklarna som används för att kryptera data, vilket gör att data inte kan användas. Det finns inget sätt att återskapa enhetsdata efter en kryptografisk radering, vidare inaktiveras dataskyddet för den självkrypterande enheten och enheten är klar för att användas för ett annat syfte.

Obs!

- Om det inträffar ett fel i hanteringsfunktionerna för en självkrypterande enhet bör du stänga av datorn helt (inte med alternativet Starta om) och starta den igen.
- Om du vill veta mer om ett visst felmeddelande kan du gå till wave.com/support/Dell.

Information om enhet för autentisering

I fönstret Enhet för autentisering i **Enhetshantering** visas information om och status för alla anslutna enheter för autentisering (dvs. fingeravtrycksläsare, traditionella eller så kallade contactless smartcard-läsare) i systemet.

Teknisk support

Teknisk support för programvaran **Dell dataskydd | Åtkomst** finns på http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP

Kryptografiprovidern (CSP) Wave Systems Trusted Computing Group (TCG)-enabled CSP medföljer programmet **Dell dataskydd | Åtkomst** och kan användas när du behöver en CSP – antingen genom ett direktanrop från ett program eller genom att du väljer det från en lista med installerade CSPer. Du bör om möjligt välja ”Wave TCG-Enabled CSP” för att säkerställa att TPM genererar nycklarna, och att nycklarna med tillhörande lösenord hanteras av **Dell dataskydd | Åtkomst**.

Wave Systems TCG-enabled CSP gör det möjligt för program att använda funktioner på plattformar som utformats enligt TCG-standarden direkt via MSCAPI. Det är en TCG-förstärkt MSCAPI CSP-modul som tillhandahåller assymetriska nyckelfunktioner på TPM och som vidareutvecklar de avancerade säkerhetsfunktionerna i TPM och fungerar oberoende av systemspecifika krav på TSS-provider (Trusted Software Stack).

Obs! Om TPM-nycklarna som skapats av Wave TCG-enabled CSP kräver lösenord och användaren har skapat ett TPM-huvudlösenord kommer de enskilda nyckellösenorden att genereras slumpmässigt och lagras i lösenordsarkivet i TPM.