Startpagina Dell Data Protection | Access

De startpagina **Dell Data Protection | Access** is het beginpunt voor toegang tot de functies van deze toepassing. In dit venster krijgt u toegang tot:

System Access Wizard
Access Opties
Self-Encrypting Drive
Geavanceerde opties

In de rechterbenedenhoek van het venster vindt u de koppeling **Geavanceerd** waarop u kunt klikken voor toegang tot geavanceerde opties.

In het venster met de geavanceerde opties kunt u in de rechterbenedenhoek op de koppeling **Startpagina** klikken om terug te keren naar de startpagina.

System Access Wizard

De System Access Wizard start automatisch de eerste keer dat de toepassing **Dell Data Protection | Access** wordt gestart. Deze wizard begeleidt u bij het instellen van alle aspecten van de beveiliging op uw systeem, inclusief hoe (bijvoorbeeld alleen wachtwoord of vingerafdruk en wachtwoord) en wanneer (bij Windows-aanmelding, pre-Windows-aanmelding of beide) u zich bij het systeem wilt aanmelden. Als uw systeem bovendien een Self-Encrypting Drive heeft, kunt u dit station ook met deze wizard configureren.

Beheerdersfuncties

Gebruikers waarvoor in het systeem Windows-beheerdersbevoegdheden zijn ingesteld, hebben de nodige rechten om in **Dell Data Protection | Access** de volgende functies uit te voeren, die standaardgebruikers niet kunnen uitvoeren:

- Systeemwachtwoord (Pre-Windows) instellen/wijzigen
- Wachtwoord van vaste schijf instellen/wijzigen
- Beheerderswachtwoord instellen/wijzigen
- Wachtwoord voor TPM-eigendom instellen/wijzigen
- ControlVault-beheerderswachtwoord instellen/wijzigen
- Systeem opnieuw instellen
- Referenties archiveren en herstellen
- PIN voor beheerder voor smartcard instellen/wijzigen
- Smartcard wissen/opnieuw instellen
- Dell Beveiligde aanmelding voor Windows inschakelen/uitschakelen
- Windows-aanmeldingsbeleid instellen
- Self-Encrypting Drives beheren, alsook:
    - Vergrendeling van Self-Encrypting Drive inschakelen/uitschakelen
    - Windows Wachtwoordsynchronisatie inschakelen/uitschakelen
    - Single Sign On (SSO) inschakelen/uitschakelen
    - Cryptografisch wissen

Extern beheer

Uw organisatie kan een omgeving instellen waarin de beveiligingsfuncties van de toepassing **Dell Data Protection | Access** op meerdere platforms centraal worden beheerd (extern beheer). In dat geval kan een Windows-beveiligingsinfrastructuur zoals Active Directory worden gebruikt om specifieke functies van **Dell Data Protection | Access** op veilige wijze te beheren.

Wanneer een computer extern wordt beheerd (bijvoorbeeld als deze eigendom is van de externe beheerder), is lokaal beheer van de **Dell Data Protection | Access**-functionaliteit uitgeschakeld. De beheervensters van de toepassing zijn lokaal niet toegankelijk. Beheer van de volgende functies vindt extern plaats:

- Trusted Platform Module (TPM)
- ControlVault
- Pre-Windows-aanmelding
- Systeem opnieuw instellen
- BIOS-wachtwoorden
- Windows-aanmeldingsbeleid
- Self-Encrypting Drives
- Inschrijving van vingerafdrukken en smartcards

Neem contact op met uw Dell-vertegenwoordiger of ga naar dell.com voor meer informatie over het gebruik van Wave Systems EMBASSY® Remote Administration Server (ERAS) voor extern beheer.

Access Opties

In het venster Access Opties kunt u instellen hoe u toegang tot uw systeem krijgt.

Als u opties voor **Dell Data Protection | Access** hebt ingesteld, worden deze op de startpagina weergegeven met de beschikbare opties (bijvoorbeeld wachtwoord wijzigen voor Pre-Windows-aanmelding). De beschikbare opties zijn snelkoppelingen waarop u kunt klikken om naar het desbetreffende venster te gaan waarin u een specifieke taak kunt uitvoeren (bijvoorbeeld uw pre-Windows-wachtwoord wijzigen of een andere vingerafdruk inschrijven).

Algemeen
U kunt eerst opgeven wanneer (Windows, pre-Windows of beide) en hoe (vingerafdruk en/of wachtwoord) u zich wilt aanmelden. U kunt kiezen uit een of twee aanmeldingsopties, waaronder combinaties met vingerafdruk, smartcard en wachtwoord. De weergegeven opties zijn gebaseerd op het aanmeldingsbeleid in uw omgeving en wat op het platform wordt ondersteund.

Vingerafdruk
Als uw systeem een vingerafdruklezer bevat, kunt u vingerafdrukken inschrijven of bijwerken voor gebruik bij aanmelding op uw systeem. Wanneer u vingerafdrukken hebt ingeschreven, kunt u de ingeschreven vinger(s) over de vingerafdruklezer van uw systeem bewegen om toegang te krijgen tot uw systeem bij Windows-aanmelding, pre-Windows-aanmelding of beide (afhankelijk van de geselecteerde instelling in de algemene toegangsopties). Zie Vingerafdrukken van gebruikers inschrijven voor meer informatie.

Pre-Windows-aanmelding
Als u hebt opgegeven dat gebruikers zich pre-Windows dienen aan te melden, moet u een systeemwachtwoord (soms ook wel het pre-Windows-wachtwoord genoemd) instellen voor pre-Windows-toegang. Zodra dit is ingesteld, kan de beheerder het wachtwoord op elk gewenst moment wijzigen.

U kunt in dit scherm pre-Windows-aanmelding ook uitschakelen. Hiertoe dient u uw huidige systeemwachtwoord in te voeren, het wachtwoord te bevestigen en vervolgens op de knop **Uitschakelen** te klikken.

Smartcard
Als u hebt opgegeven dat gebruikers zich met een smartcard aanmelden, moet u een of meer traditionele (contacted) of contactless smartcards inschrijven. Klik op de koppeling **Andere smartcard inschrijven** om de inschrijvingswizard voor smartcards te starten. Inschrijving houdt in dat u uw smartcard instelt voor gebruik bij aanmelding.

Wanneer u een smartcard hebt ingeschreven, kunt u een PIN voor die kaart wijzigen of instellen met de koppeling **PIN van mijn smartcard wijzigen of instellen** (Change or setup my smartcard PIN).

Pre-Windows-aanmelding

Wanneer pre-Windows-aanmelding is ingesteld, moet u worden geverifieerd (wachtwoord, vingerafdruk of smartcard) wanneer het systeem wordt ingeschakeld, voordat Windows wordt geladen. De pre-Windows-aanmeldingsfunctionaliteit biedt extra beveiliging voor het systeem, door te voorkomen dat onbevoegden Windows misbruiken en toegang krijgen tot de computer (bijvoorbeeld wanneer deze is gestolen).

In het venster Pre-Windows-aanmelding (Pre-Windows Login) kunnen beheerders pre-Windows-aanmelding instellen of een pre-Windows-(systeem)wachtwoord maken of wijzigen. Als het wachtwoord al is ingesteld, kunt u pre-Windows-aanmelding in dit venster uitschakelen. Als u pre-Windows-aanmelding instelt, wordt een wizard gestart waarin de volgende stappen worden voltooid:

- Systeemwachtwoord: u stelt een systeemwachtwoord in (ook wel een pre-Windows-wachtwoord genoemd) voor pre-Windows-toegang. Dit wachtwoord wordt ook als back-up gebruikt in de gevallen dat een gebruiker extra verificatieniveaus heeft (bijvoorbeeld om toegang te krijgen tot het systeem als er een probleem is met de vingerafdruksensor).
- Vingerafdruk of smartcard: u stelt een vingerafdruk of smartcard in voor gebruik bij pre-Windows-aanmelding en geeft u op of dit verificatieniveau wordt gebruikt in plaats van, of als aanvulling op, het pre-Windows-wachtwoord.
- Single Sign On: uw pre-Windows-verificatie (wachtwoord, vingerafdruk of smartcard) wordt standaard gebruikt om u tevens automatisch bij Windows aan te melden (dit wordt "Single Sign On" genoemd). Als u deze functie wilt uitschakelen, schakelt u het selectievakje Ik wil mij opnieuw bij Windows aanmelden (I want to login again at Windows) in.
- Als een BIOS-wachtwoord van de vaste schijf wordt ingesteld als aanvulling op een pre-Windows-wachtwoord, hebt u tevens de optie om het wachtwoord van de vaste schijf te wijzigen of uit te schakelen.

Opmerking: niet alle vingerafdruklezers zijn geschikt voor gebruik met pre-Windows-verificatie. Als uw lezer niet compatibel is, kunt u vingerafdrukken alleen inschrijven voor Windows-aanmelding. Als u wilt weten of een specifieke vingerafdruklezer compatibel is, neemt u contact op met uw systeembeheerder of gaat u naar support.dell.com voor een lijst met ondersteunde vingerafdruklezers.

Pre-Windows-aanmelding uitschakelen
U kunt in dit venster pre-Windows-aanmelding ook uitschakelen. Hiertoe dient u uw huidige pre-Windows-(systeem)wachtwoord in te voeren, het wachtwoord te bevestigen en vervolgens op de knop **Uitschakelen** te klikken. Wanneer u pre-Windows-aanmelding uitschakelt, blijven ingeschreven vingerafdrukken of smartcards ingeschreven.

Vingerafdrukken inschrijven/verwijderen

Gebruikers kunnen vingerafdrukken inschrijven of bijwerken die door het systeem kunnen worden gebruikt voor verificatie bij pre-Windows- of Windows-aanmelding. Op het tabblad Vingerafdruk wordt met afbeeldingen van handen weergegeven welke vingers zijn ingeschreven. Als u op de koppeling **Andere vinger inschrijven** klikt, wordt de wizard Vingerafdruk inschrijven gestart die u door het inschrijvingsproces leidt. Inschrijving houdt in dat een vingerafdruk wordt opgeslagen voor gebruik bij aanmelding. Voor de inschrijving van vingerafdrukken moet een geldige vingerafdruklezer zijn geïnstalleerd en geconfigureerd.

Opmerking: niet alle vingerafdruklezers kunnen voor pre-Windows-aanmelding worden gebruikt. Als u een vingerafdruk voor pre-Windows probeert in te schrijven met een incompatibele lezer, verschijnt een foutbericht. Als u wilt weten of het apparaat compatibel is, neemt u contact op met uw systeembeheerder of gaat u naar support.dell.com voor een lijst met ondersteunde vingerafdruklezers.

Wanneer u vingerafdrukken inschrijft, wordt u gevraagd om uw Windows-wachtwoord in te voeren om uw identiteit te controleren. Als uw beleid dit vereist, wordt u tevens gevraagd om uw Pre-Windows-(systeem)wachtwoord in te voeren. Het Pre-Windows-wachtwoord kan worden gebruikt om toegang te krijgen tot het systeem als u problemen ondervindt met de vingerafdruklezer.

Opmerkingen:

- U wordt aanbevolen bij het inschrijvingsproces minimaal twee vingerafdrukken in te schrijven.
- U moeten ervoor zorgen dat vingerafdrukken correct zijn ingeschreven voordat u de mogelijkheden van vingerafdrukverificatie inschakelt.
- Als u vingerafdruklezers op een systeem wijzigt, moet u vingerafdrukken opnieuw inschrijven met de nieuwe lezer. Het verdient geen aanbeveling heen en weer te schakelen tussen twee verschillende vingerafdruklezers.
- Als berichten zoals "Sensor heeft focus verloren" verschijnen wanneer u vingerafdrukken inschrijft, houdt dit in dat de computer de vingerafdruklezer niet herkent. Als u een externe vingerafdruklezer gebruikt, kunt u het probleem vaak oplossen door de vingerafdruklezer los te koppelen en vervolgens weer aan te sluiten.

Ingeschreven vingerafdrukken wissen

U kunt ingeschreven vingerafdrukken verwijderen door de op de koppeling **Vinger verwijderen** te klikken of door op een ingeschreven vinger te klikken in de wizard Vingerafdruk inschrijven.

Om een specifieke gebruiker te verwijderen die vingerafdrukken heeft ingeschreven voor pre-Windows-verificatie, kan de beheerder alle vingerafdrukken deselecteren die voor die gebruiker zijn ingeschreven.

Opmerking: als tijdens het inschrijvingsproces voor vingerafdrukken fouten optreden, gaat u naar wave.com/support/Dell voor meer details.

Smartcards inschrijven

Dell Data Protection | Access biedt u de optie om een traditionele (contacted) of contactless smartcard te gebruiken voor aanmelding bij uw Windows-account of voor pre-Windows-verificatie. Klik op het tabblad Smartcard op de koppeling **Andere smartcard inschrijven** om de wizard Inschrijven voor smartcards te starten die u door het inschrijvingsproces leidt. Inschrijving houdt in dat u uw smartcard instelt voor gebruik bij aanmelding.

Voor de inschrijving moet een geldig smartcardverificatieapparaat zijn geïnstalleerd en geconfigureerd.

Opmerking: als u wilt weten of een bepaald apparaat compatibel is, neemt u contact op met uw systeembeheerder of gaat u naar support.dell.com voor een lijst met ondersteunde smartcards.

Inschrijving
Wanneer u een smartcard inschrijft, wordt u gevraagd om uw Windows-wachtwoord in te voeren om uw identiteit te controleren. Als uw beleid dit vereist, wordt u tevens gevraagd om uw Pre-Windows-(systeem)wachtwoord in te voeren. Het Pre-Windows-wachtwoord kan worden gebruikt om toegang te krijgen tot het systeem als u problemen ondervindt met de smartcardlezer.

Tijdens de inschrijving wordt u gevraagd om de smartcard-PIN in te voeren, als deze is ingesteld. Als uw beleid een PIN vereist, maar geen PIN is ingesteld, wordt u gevraagd om een PIN te maken.

Opmerkingen:

- Wanneer een gebruiker is ingeschreven voor gebruik van een smartcard bij pre-Windows-aanmelding, kan hij of zij niet worden verwijderd.
- Standaardgebruikers kunnen de gebruikers-PIN op een smartcard wijzigen en de beheerder kan zowel de beheerders-PIN als de gebruikers-PIN wijzigen.
- De beheerder kan een smartcard bovendien opnieuw instellen. Daarna kan de smartcard niet worden gebruikt voor verificatie bij Windows- of pre-Windows-aanmelding totdat deze opnieuw is ingeschreven.

Opmerking:voor TPM-certificaatverificatie kunnen beheerders TPM-certificaten inschrijven via het Microsoft Windows-inschrijvingsproces voor smartcards. Beheerders moeten Wave TCG Enabled CSP als de cryptografieprovider (CSP) in plaats van een Smartcard CSP selecteren voor compatibiliteit met deze toepassing. Daarenboven moet Dell Beveiligde aanmelding zijn ingeschakeld met het geschikte beleid voor verificatietypen voor de client.

Opmerking: als in een foutbericht wordt gemeld dat de smartcardservice niet actief is, kunt u deze service als volgt (her)starten:

- Navigeer in het Configuratiescherm naar Systeembeheer, selecteer Services, klik met de rechtermuisknop op Smartcard en selecteer Starten of Opnieuw starten.
- Bezoek wave.com/support/Dell voor meer gedetailleerde informatie over een specifiek foutbericht.

Self-Encrypting Drive

Dell Data Protection | Access beheert de hardwaregebaseerde beveiligingsfuncties van Self-Encrypting Drives, waarop gegevensversleuteling in de stationshardware is ingesloten. Deze functionaliteit wordt gebruikt om te garanderen dat alle bevoegde gebruikers toegang krijgen tot versleutelde gegevens (wanneer de stationsvergrendeling is ingeschakeld).

U krijgt toegang tot het venster Self-Encrypting Drive door onderaan op de tab **Self-Encrypting Drive** te klikken. Deze tab wordt alleen weergegeven wanneer een of meer Self-Encrypting Drives (SED's) aanwezig zijn op uw systeem.

Klik op de koppeling **Instellen** (Setup) als u de wizard Self-Encrypting Drive instellen (Self-Encrypting Drive Setup Wizard) wilt starten. In deze wizard maakt u het wachtwoord van de stationsbeheerder, maakt u een back-up van dit wachtwoord en past u uw instellingen voor de stationsversleuteling toe. Alleen systeembeheerders krijgen toegang tot de wizard Self-Encrypting Drive (Self-Encrypting Drive Setup Wizard) instellen.

Belangrijk: wanneer het station is ingesteld, zijn gegevensbeveiliging en stationsvergrendeling "ingeschakeld". Wanneer een station is vergrendeld, is het volgende gedrag van toepassing:

- De *vergrendelde* modus van het station treedt in werking zodra het station wordt uitgeschakeld.
- Het station zal pas worden opgestart nadat de gebruiker de juiste gebruikersnaam en het juiste wachtwoord (of vingerafdruk) heeft ingevoerd in het Pre-Windows-aanmeldingsscherm. Voordat stationsvergrendeling wordt ingeschakeld, zijn de gegevens op het station toegankelijk voor elke gebruiker op de computer.
- Het station is beveiligd ook als dit als een secundair station op een andere computer is aangesloten. Verificatie is vereist voor toegang tot de stationsgegevens.

Wanneer het station is ingesteld, worden in het venster Self-Encrypting Drive een of meer stations weergegeven alsook een koppeling waarmee gebruikers hun stationswachtwoord kunnen wijzigen. Als u een stationsbeheerder bent, kunt u in dit venster ook stationsgebruikers toevoegen of verwijderen. Als een extern station is ingesteld, wordt het in dit venster weergegeven zodat het kan worden ontgrendeld.

Opmerking: als u een secundair, extern station wilt vergrendelen, moet het station los van de computer worden uitgeschakeld.

De stationsbeheerder kan de stationsinstellingen beheren in **Geavanceerd>Apparaten** (Advanced>Devices). Zie Apparaatbeheer - Self-Encrypting Drives voor meer informatie.

Station instellen

De wizard Self-Encrypting Drive instellen (Self-Encrypting Drive Setup Wizard) leidt u door het instellingsproces voor uw station(s). De volgende concepten zijn belangrijk wanneer u dit proces doorloopt.

Stationsbeheerder

De eerste gebruiker met systeembeheerdersrechten die stationstoegang instelt (en het wachtwoord van de stationsbeheerder instelt) wordt de stationsbeheerder. Alleen deze gebruiker heeft rechten om wijzigingen te maken in schijftoegang. Om ervoor te zorgen dat de eerste gebruiker alleen als de stationsbeheerder wordt ingesteld als dit de bedoeling is, moet u het selectievakje "Ik begrijp" (I understand) inschakelen om door te gaan met deze stap.

Wachtwoord van stationsbeheerder
In de wizard wordt u gevraagd om het wachtwoord van de stationsbeheerder te maken en vervolgens opnieuw in te voeren als bevestiging. U moet uw Windows-wachtwoord invoeren om uw identiteit te bevestigen voordat u uw wachtwoord van stationsbeheerder kunt maken. De huidige Windows-gebruiker moet beheerdersrechten hebben om dit wachtwoord te maken.

Back-up van stationsreferenties maken
Typ een locatie of klik op de knop **Bladeren** om een locatie te selecteren waar u de back-up van uw referenties van stationsbeheerder wilt opslaan.

Belangrijk**:**

- U wordt sterk aanbevolen een back-up van deze referenties te maken naar een ander station dan uw primaire vaste schijf (bijvoorbeeld een verwijderbaar medium). Als u toegang tot uw vaste schijf verliest, hebt u anders ook geen toegang meer tot uw back-up.
- Wanneer u het station hebt ingesteld, moetelke gebruiker de juiste gebruikersnaam en het bijbehorende wachtwoord (of een vingerafdruk) invoeren voordat Windows wordt geladen, om toegang te krijgen tot het systeem de volgende keer dat het systeem wordt ingeschakeld.

Stationsgebruiker toevoegen
De stationsbeheerder kan aan het station gebruikers toevoegen die geldige Windows-gebruikers zijn. Wanneer de beheerder gebruikers aan het station toevoegt, kan hij of zij een optie instellen om de gebruikers te vragen het wachtwoord opnieuw in te stellen de eerste keer zij zich aanmelden. De gebruikers moeten hun wachtwoord vervolgens opnieuw instellen in het pre-Windows-verificatiescherm voordat het station wordt ontgrendeld.

Geavanceerde instellingen

- *Single Sign On* - Uw Self-Encrypting Drive-wachtwoord dat u pre-Windows invoert voor verificatie op het station, wordt tevens gebruikt om u automatisch aan te melden bij Windows (dit wordt "Single Sign On" genoemd). Als u deze functie wilt uitschakelen, schakelt u het selectievakje "Ik wil mij opnieuw aanmelden wanneer Windows start" (I want to login again when Windows starts) in wanneer u uw stationsinstellingen configureert.
- *Aanmelding met vingerafdruk* - Op ondersteunde platforms kunt u opgeven dat u voor verificatie op uw Self-Encrypting Drive een vingerafdruk in plaats van een wachtwoord wilt gebruiken.
- *Ondersteuning voorSlaapstand/stand-by (S3)* (indien ondersteund op het platform) - Indien ingeschakeld, kan uw Self-Encrypting Drive op veilige wijze in de slaapstand of stand-by (ook wel S3-modus genoemd) worden gezet. Daarna is pre-Windows-verificatie vereist wanneer de computer uit de slaapstand of stand-by wordt gehaald.

Opmerkingen:

- Wanneer de ondersteuning voor S3 is ingeschakeld, zijn wachtwoorden voor stationsversleuteling onderhevig aan eventuele beperkingen voor BIOS-wachtwoorden. Neem contact op met de fabrikant van de systeemhardware voor meer informatie over alle specifieke beperkingen voor het BIOS-wachtwoord die mogelijk voor het systeem bestaan.
- Niet alle Self-Encrypting Drives ondersteunen de S3-modus. Tijdens het instellen van het station wordt gemeld of het station slaapstand of stand-by ondersteunt. Voor stations die deze modus niet ondersteunen, worden Windows S3-verzoeken automatisch geconverteerd naar sluimerstandverzoeken, als de sluimerstand is ingeschakeld. (U wordt sterk aanbevolen om de sluimerstand op uw computer in te schakelen).
- De eerste keer dat u zich aanmeldt nadat de optie Single Sign On (SSO) is ingesteld, wordt het proces onderbroken bij de Windows-aanmeldingsprompt. U dient uw vorm van Windows-verificatie in te voeren, die vervolgens veilig zal worden opgeslagen voor toekomstige Windows-aanmeldingspogingen. De volgende keer dat het systeem wordt opgestart, wordt u door SSO automatisch bij Windows aangemeld. Hetzelfde proces is ook

vereist wanneer de Windows-verificatie van een gebruiker (wachtwoord, vingerafdruk, PIN voor smartcard) verandert. Als de computer zich in een domein bevindt en dat domein een beleid heeft waarvoor Ctrl+Alt+Del moet worden ingedrukt voor aanmelding bij Windows, wordt dit beleid nageleefd.

Waarschuwing:als u de installatie van de toepassing **Dell Data Protection | Access** ongedaan maakt, moet u eerst de Self-Encrypting Drive-gegevensbeveiliging uitschakelen en het station ontgrendelen.

Gebruikersfuncties van Self-Encrypting Drive

Beheerders van Self-Encrypting Drives voeren het volledige beheer van de stationsbeveiliging en de gebruikers uit. Stationsgebruikers die geen stationsbeheerder zijn, kunnen alleen de volgende taken uitvoeren:

- Hun eigen stationswachtwoord wijzigen
- Een station ontgrendelen

Deze taken zijn toegankelijk vanaf het tabblad **Self-Encrypting Drive** in **Dell Data Protection | Access**.

Wachtwoord wijzigen
Ingeschreven gebruikers kunnen een nieuw verificatiewachtwoord voor het station maken. U moet uw huidige Self-Encrypting Drive-wachtwoord invoeren voordat het stationswachtwoord op de nieuwe waarde wordt ingesteld.

Opmerkingen:

- De toepassing dwingt de lengte van het Windows-wachtwoord en de beleidsregels voor de complexiteit van Windows-wachtwoorden af, indien die zijn ingeschakeld. Als geen beleid voor Windows-wachtwoorden is ingeschakeld, mag het Self-Encrypting Drive-wachtwoord maximaal 32 tekens lang zijn. De maximumlengte is 127 tekens als S3 (slaapstand/stand-by) niet is ingeschakeld.
- Het Self-Encrypting Drive-wachtwoord van een gebruiker is onafhankelijk van zijn of haar Windows-wachtwoord. Wanneer het Windows-wachtwoord van een gebruiker wordt gewijzigd of opnieuw wordt ingesteld, heeft dit geen invloed op het stationswachtwoord van die gebruiker, tenzij Windows Wachtwoordsynchronisatie is ingeschakeld. Zie Apparaten: Self-Encrypting Drives voor details.
- Sommige niet-Engelse toetsenborden hebben een aantal beperkte tekens die niet in het Self-Encrypting Drive-wachtwoord mogen worden gebruikt. Als het Windows-wachtwoord een van de beperkte tekens bevat en Windows Wachtwoordsynchronisatie is ingeschakeld, kan de synchronisatie niet worden voltooid en verschijnt een foutbericht.

Station ontgrendelen
Een ingeschreven stationsgebruiker kan een vergrendeld station ontgrendelen. Als de stationsvergrendeling is ingeschakeld, treedt de vergrendelde toestand van het station in werking wanneer de computer wordt uitgeschakeld. Wanneer het systeem opnieuw wordt ingeschakeld, moet u zich voor het station verifiëren door uw wachtwoord in het pre-Windows-verificatiescherm in te voeren.

Opmerkingen:

- Als meerdere Self-Encrypting Drive-gebruikersaccounts gelijktijdig actief zijn op een computer, is het mogelijk dat de energiespaarstand (slaapstand, stand-by of sluimerstand) niet in werking kan treden.
- In de volgende taalversies van de toepassing wordt in het pre-Windows-verificatiescherm Gebruiker 1, Gebruiker 2, enz. vervangen door de namen van de stationsgebruikers: Chinees, Japans, Koreaans en Russisch.

Geavanceerde opties

Met de geavanceerde opties in **Dell Data Protection | Access** kan een gebruiker met beheerdersbevoegdheden de volgende aspecten van de toepassing beheren:

Onderhoud
Wachtwoorden
Apparaten

Opmerking: alleen gebruikers met beheerdersbevoegdheden kunnen wijzigingen in de geavanceerde opties maken. Standaardgebruikers kunnen deze instellingen weergeven, maar niet wijzigen.

Overzicht van onderhoud

In het venster Onderhoud (Maintenance) kunnen beheerders Windows-aanmeldingsvoorkeuren instellen, een systeem opnieuw instellen om het voor te bereiden als u de computer een nieuwe bestemming wilt geven, of gebruikersreferenties archiveren of herstellen die in de beveiligingshardware van het systeem zijn opgeslagen. Zie de volgende onderwerpen voor details:

Access Voorkeuren
Systeem opnieuw instellen
Referenties archiveren en herstellen

Access Voorkeuren

In het venster Access Voorkeuren kunnen beheerders Windows-aanmeldingsvoorkeuren voor alle gebruikers van het systeem opgeven.

Dell Beveiligde aanmelding inschakelen
De optie waarmee u het Windows ctrl-alt-delete-standaardvenster kunt vervangen, biedt u de mogelijkheid om verschillende verificatieniveaus te gebruiken in plaats van (of als aanvulling op) het Windows-wachtwoord voor toegang tot Windows. U kunt een vingerafdruk als tweede verificatieniveau toevoegen om de beveiliging van het Windows-aanmeldingsproces te verhogen. U kunt ook nog andere verificatieniveaus toevoegen voor aanmelding bij Windows, bijvoorbeeld een smartcard of een TPM-certificaat.

Opmerkingen:

- Het inschakelen van Dell Beveiligde aanmelding is van invloed op alle gebruikers van het systeem.
- U wordt aanbevolen deze optie slechts in te schakelen NADAT gebruikers hun vingerafdrukken of smartcard hebben ingeschreven.
- De eerste keer dat u zich aanmeldt nadat deze optie is ingesteld, wordt u gevraagd de verificatie voor Windows uit te voeren volgens uw standaardbeleid en vervolgens dient u uw nieuwe verificatieniveaus te gebruiken de volgende keer dat u opstart.

Dell Beveiligde aanmelding uitschakelen
Met deze optie worden alle functies van **Dell Data Protection | Access** voor aanmelding bij Windows uitgeschakeld. Wanneer deze optie is geselecteerd, wordt het standaardaanmeldingsbeleid van Windows opnieuw van kracht.

Opmerkingen:

- Als een foutbericht verschijnt over beveiligde Windows-aanmelding wanneer u probeert aan te melden, schakelt u de optie Dell Beveiligde aanmelding uit en vervolgens weer in.
- Bezoek wave.com/support/Dell voor meer gedetailleerde informatie over een specifiek foutbericht.

Systeem opnieuw instellen

De functie Systeem opnieuw instellen wordt gebruikt om alle gebruikersgegevens van alle beveiligingshardware op het platform te wissen, bijvoorbeeld wanneer een computer een nieuwe bestemming krijgt. Met deze optie worden alle wachtwoorden in het systeem gewist, met uitzondering van de Windows-gebruikerswachtwoorden, alsook alle gegevens in de hardwareapparaten (ControlVault, TPM en vingerafdruklezers). Voor Self-Encrypting Drives schakelt u met deze functie ook gegevensbeveiliging uit, waardoor de gegevens op de drive toegankelijk zijn.

U dient te bevestigen dat u begrijpt dat u het systeem opnieuw instelt en vervolgens klikt u op **Volgende**. Als u het systeem opnieuw wilt instellen, moet u voor elk beveiligingsapparaat het wachtwoord, indien ingesteld, invoeren:

- TPM-eigendom
- ControlVault-beheerder
- BIOS-beheerder
- BIOS-systeem (pre-Windows)
- Vaste schijf (BIOS)
- Self-Encrypting Drive-beheerder

Opmerking: voor Self-Encrypting Drives is alleen het wachtwoord van de stationsbeheerder vereist, niet de wachtwoorden van alle stationsgebruikers.

Belangrijk: u kunt gegevens die zijn gewist tijdens het opnieuw instellen van het systeem, alleen terughalen door een eerder opgeslagen archief te herstellen. Als u geen archief hebt, zijn deze gegevens voorgoed verloren. Voor een Self-Encrypting Drive worden alleen de instellingsgegevens verwijderd. Op het station worden geen persoonlijke gegevens verwijderd.

Referenties archiveren en herstellen

De functionaliteit Referenties archiveren en herstellen wordt gebruikt om back-ups te maken van alle gebruikersreferenties (aanmeldings- en versleutelingsinformatie) die in de ControlVault en Trusted Platform Module (TPM) zijn opgeslagen en deze zo nodig te herstellen. Een back-up van deze gegevens is belangrijk wanneer een computer opnieuw wordt ingericht of gegevens moeten worden hersteld nadat een hardwarestoring is opgetreden. In dit geval kunt u al uw referenties eenvoudig naar uw nieuwe computer herstellen vanaf een opgeslagen, gearchiveerd bestand.

U hebt de keuze om referenties voor één gebruiker of voor alle gebruikers op het systeem te archiveren of te herstellen.

De gebruikersreferenties bestaan uit gegevens die worden gebruikt voor pre-Windows-aanmelding, zoals ingeschreven vingerafdrukken en smartcardgegevens, en sleutels die in de TPM zijn opgeslagen. De TPM maakt sleutels op verzoek van beveiligingstoepassingen. Zo worden tijdens het genereren van een digitaal certificaat bijvoorbeeld sleutels in de TPM gemaakt.

Opmerking: als u wilt weten of **Dell Data Protection | Access** de TPM-sleutels kan archiveren, raadpleegt u de documentatie voor de beveiligde toepassing. Over het algemeen worden alle toepassingen ondersteund die sleutels genereren met behulp van de Wave TCG Enabled CSP.

Referenties archiveren
U kunt als volgt referenties archiveren:

- Geef op of u referenties voor uzelf of alle gebruikers in het systeem wilt archiveren.
- Voer de verificatie voor de beveiligingshardware uit door het systeemwachtwoord (pre-Windows), het ControlVault-beheerderswachtwoord en het wachtwoord voor TPM-eigendom in te voeren.
- Maak een wachtwoord voor de back-up van de referenties.
- Geef een archieflocatie op met de knop **Bladeren**. De archieflocatie moet een verwijderbaar medium zijn, zoals een USB-flashstation of netwerkstation, als bescherming tegen een storing van een vaste schijf.

Belangrijke opmerkingen:
- Noteer de archieflocatie. De gebruiker heeft deze informatie nodig om de referentiegegevens te herstellen.
- Noteer ook het wachtwoord voor de back-up van de referenties zodat de gegevens later kunnen worden hersteld. Dit is belangrijk omdat het wachtwoord niet kan worden hersteld.
- Als u het wachtwoord voor TPM-eigendom niet weet, neemt u contact op met de systeembeheerder of raadpleegt u de installatie-instructies van de TPM van de computer.

Referenties herstellen
U kunt als volgt referenties herstellen:

- Geef op of u referenties voor uzelf of alle gebruikers in het systeem wilt herstellen.
- Blader naar de archieflocatie en selecteer het archiefbestand.
- Voer het wachtwoord voor de back-up van de referenties in dat u hebt gemaakt tijdens het instellen van het archief.
- Voer de verificatie voor de beveiligingshardware uit door het systeemwachtwoord (pre-Windows), het ControlVault-beheerderswachtwoord en het wachtwoord voor TPM-eigendom in te voeren.

Opmerkingen:

- Als in een foutbericht wordt gemeld dat het herstellen van de referenties is mislukt en u meerdere keren hebt geprobeerd om een herstelling uit te voeren, probeert u een ander archiefbestand te herstellen. Als ook die poging mislukt, maakt u een ander archiefbestand met referenties en probeert u het nieuwe archiefbestand te herstellen.
- Als in een foutbericht wordt gemeld dat TPM-sleutels niet kunnen worden hersteld, maakt u een archiefbestand met referenties en wist u vervolgens de TPM in het BIOS. Als u de TPM wilt wissen, start u uw computer opnieuw op, drukt u tijdens het opstarten op de **F2**-toets voor toegang tot de BIOS-instellingen en navigeert u vervolgens naar Security>TPM Security. Stel vervolgens de eigendom van de TPM opnieuw in en probeer de referenties nogmaals te herstellen.
- Bezoek wave.com/support/Dell voor meer gedetailleerde informatie over een specifiek foutbericht.

Wachtwoordbeheer

In het venster Wachtwoordbeheer kan een beheerder alle beveiligingswachtwoorden in uw systeem maken of wijzigen:

- Systeem (ook bekend als Pre-Windows)*
- Beheerder*
- Vaste schijf*
- ControlVault
- TPM-eigendom
- TPM-hoofd
- TPM-wachtwoordenkluis
- Self-Encrypting Drive

Opmerkingen:

- Alleen de wachtwoorden die van toepassing zijn op de huidige platformconfiguratie worden weergegeven. Dit venster verandert dus afhankeijk van de configuratie en status van het systeem.
- De bovenstaande wachtwoordtypen die met een * zijn gemarkeerd, zijn BIOS-wachtwoorden en kunnen ook via het systeem-BIOS worden gewijzigd.
- De wachtwoorden op BIOS-niveau kunnen niet worden gemaakt of gewijzigd als de BIOS-beheerder wachtwoordwijzigingen heeft geweigerd
- Als u op de koppeling **Instellen** (Setup) voor een Self-Encrypting Drive klikt, wordt de wizard Self-Encrypting Drive instellen (Self-Encrypting Drive setup wizard) gestart. Als u op **Beheren** klikt, kunt u een of meer Self-Encrypting Drive-wachtwoorden wijzigen.
- Als u op de koppeling **Beheren** voor de TPM-wachtwoordenkluis klikt, wordt een venster weergegeven waarin u de wachtwoorden kunt weergeven of wijzigen die uw TPM-sleutels beveiligen. Wanneer een TPM-sleutel wordt gemaakt waarvoor een wachtwoord is vereist, wordt een willekeurig gegenereerd wachtwoord maakt en in de kluis geplaatst. U kunt de TPM-wachtwoordenkluis niet beheren tot u een TPM-hoofdwachtwoord hebt gemaakt.

Regels voor de complexiteit van Windows-wachtwoorden

Dell Data Protection | Access zorgt ervoor dat het volgende wachtwoord voldoet aan de regels voor de complexiteit van Windows-wachtwoorden voor de computer:

- Wachtwoord voor TPM-eigendom

Als u het beleid voor de complexiteit van Windows-wachtwoorden voor een computer wilt bepalen, volgt u deze stappen:

1. Open het Configuratiescherm.
2. Dubbelklik op Systeembeheer.
3. Dubbelklik op Lokaal beveiligingsbeleid.
4. Vouw Accountbeleid uit en selecteer Wachtwoordbeleid.

Overzicht van apparaten

Het venster Apparaten (Devices) wordt door beheerders gebruikt om alle beveiligingsapparaten te beheren die op hun systeem zijn geïnstalleerd. Voor elk apparaat kunt u de status en gedetailleerde informatie, zoals de firmwareversie, weergeven. Klik op **Weergeven** (Show) om de informatie voor elk apparaat weer te geven of op **Verbergen** (HIde) om die sectie samen te vouwen. De volgende apparaten kunnen indien aanwezig op uw platform worden beheerd:

Trusted Platform Module (TPM)
ControlVault®
Self-Encrypting Drive(s)
Informatie over verificatieapparaat

Trusted Platform Module (TPM)

De TPM-beveiligingschip moet zijn ingeschakeld en eigendom van de TPM moet zijn vastgelegd om de geavanceerde beveiligingsfuncties te kunnen gebruiken die beschikbaar zijn met **Dell Data Protection | Access** en de TPM.

Het venster Trusted Platform Module in **Apparaatbeheer** wordt alleen weergegeven wanneer op uw systeem een TPM is gedetecteerd.

TPM-beheer
Met deze functies kan de systeembeheerder de TPM beheren.

Status
Hier wordt de status *Actief* of *Inactief* voor de TPM weergegeven. De status "Actief" houdt in dat de TPM in het BIOS is ingeschakeld en klaar is om te worden ingesteld (eigendom kan worden ingesteld). De TPM kan niet worden beheerd en de beveiligingsfuncties zijn niet toegankelijk als de TPM niet actief (ingeschakeld) is.

Als de TPM op het systeem wordt gedetecteerd, maar niet actief (ingeschakeld) is, kunt u deze inschakelen door in dit venster op de koppeling **Activeren** (Activate) te klikken zonder het systeem-BIOS te openen. Nadat de TPM met deze functie is ingeschakeld, moet de computer opnieuw worden opgestart. Tijdens het opstarten wordt u in bepaalde gevallen mogelijk gevraagd om de wijzigingen te accepteren.

Opmerking: de mogelijkheid om de TPM in te schakelen (te activeren) vanuit deze toepassing wordt mogelijk niet op alle platforms ondersteund. Als deze functie niet wordt ondersteund, moet u de TPM in het systeem-BIOS inschakelen. Hiertoe start u uw systeem opnieuw op, drukt u op de **F2**-toets voordat Windows wordt geladen om het BIOS Setup-programma te openen en naar Security>TPM Security te navigeren en de TPM te activeren.

U kunt de TPM ook *deactiveren* door op de koppeling **Deactiveren** (Deactivate) te klikken. Als u de TPM deactiveert, is deze niet langer beschikbaar voor de geavanceerde beveiligingsfuncties. Deactivering wijzigt echter geen TPM-instellingen of verwijdert of wijzigt geen informatie of sleutels die in de TPM zijn opgeslagen.

Eigendom
Hier wordt de status van eigendom (bijvoorbeeld "eigendom") weergegeven en kunt u de TPM-eigenaar instellen of wijzigen. TPM-eigendom moet worden ingesteld voordat de bijbehorende beveiligingsfuncties beschikbaar worden. Voordat eigendom kan worden ingesteld, moet de TPM zijn ingeschakeld (geactiveerd).

Bij het instellen van de eigendom maakt de gebruiker (met beheerdersbevoegdheden) een wachtwoord voor TPM-eigendom. Nadat dit wachtwoord is gedefinieerd, is de eigendom ingesteld en is de TPM klaar voor gebruik.

Opmerking: het wachtwoord voor TPM-eigendom moet voldoen aan de regels voor de complexiteit van Windows-wachtwoorden voor uw systeem.

Belangrijk: het is belangrijk dat u het wachtwoord voor TPM-eigendom niet verliest of vergeet, omdat het nodig is voor toegang tot geavanceerde beveiligingsfuncties voor de TPM in **Dell Data Protection | Access**.

Vergrendeld
Hier wordt de status *Vergrendeld* of *Ontgrendeld* voor de TPM weergegeven. "Vergrendeling" is een beveiligingsfunctie van de TPM. De TPM wordt vergrendeld nadat een opgegeven aantal

keer een onjuist wachtwoord voor TPM-eigendom is ingevoerd. De TPM-eigenaar kan de TPM hier ontgrendelen. Hiervoor moet het wachtwoord voor TPM-eigendom worden ingevoerd.

Opmerkingen:

- Als in een foutbericht wordt gemeld dat de eigendom van de TPM niet kan worden ingesteld, wist u de TPM in het systeem-BIOS en probeert u de eigendom opnieuw in te stellen. Als u de TPM wilt wissen, start u uw computer opnieuw op, drukt u tijdens het opstarten op de **F2**-toets voor toegang tot de BIOS-instellingen en navigeert u vervolgens naar Security>TPM Security.
- Als in een foutbericht wordt gemeld dat het wachtwoord voor TPM-eigendom niet kan worden gewijzigd, archiveert u de TPM-gegevens (referenties archiveren), wist u de TPM in het BIOS, stelt u de eigendom van de TPM opnieuw in en herstelt u de TPM-gegevens (referenties herstellen).
- Bezoek wave.com/support/Dell voor meer gedetailleerde informatie over een specifiek foutbericht.

Dell ControlVault®

De Dell ControlVault® (CV) is een veilige hardwareopslagplaats voor gebruikersreferenties die worden gebruikt voor pre-Windows-aanmelding (bijvoorbeeld gebruikerswachtwoorden of ingeschreven vingerafdrukgegevens). Het venster ControlVault wordt alleen in **Apparaatbeheer** weergegeven als op uw systeem een ControlVault is gedetecteerd.

ControlVault-beheer

Met deze functies kan de systeembeheerder de ControlVault van het systeem beheren.

Status
Hier wordt de status *Actief* of *Inactief* voor de ControlVault weergegeven. De status Inactief geeft aan dat de ControlVault niet beschikbaar is voor opslag op uw systeem. Raadpleeg de Dell-systeemdocumentatie om te bepalen of uw systeem een ControlVault bevat.

Wachtwoord
Hiermee wordt aangegeven of het ControlVault-beheerderswachtwoord is ingesteld en kunt u tevens een wachtwoord instellen of wijzigen (als al een wachtwoord is ingesteld). Alleen systeembeheerders kunnen dit wachtwoord instellen of wijzigen. U kunt een ControlVault-beheerderswachtwoord als volgt instellen:

- Archiveer of herstel referenties.
- Wis gebruikersgegevens (voor alle gebruikers).

Opmerking: als een gebruiker probeert om referenties te archiveren of te herstellen en nog geen ControlVault-beheerderswachtwoord is ingesteld, wordt hij of zij gevraagd om er één te maken (mits hij of zij een beheerder is).

Ingeschreven gebruikers
Hiermee wordt aangegeven of gebruikers aanmeldingsgegevens hebben ingeschreven (bijvoorbeeld wachtwoorden, vingerafdrukken of smartcardgegevens) die momenteel in de ControlVault zijn opgeslagen.

Gebruikersgegevens wissen
De gegevens in de ControlVault moeten op een bepaald moment mogelijk worden gewist, bijvoorbeeld als gebruikers problemen ondervinden met het gebruik of de inschrijving van pre-Windows-referenties voor verificatie. Alle gegevens die in de ControlVault zijn opgeslagen, kunnen in dit venster voor één gebruiker of voor alle gebruikers worden gewist.

Het ControlVault-beheerderswachtwoord moet worden ingevoerd als u alle gebruikersgegevens op het platform wilt wissen. U wordt ook gevraagd om het systeemwachtwoord (pre-Windows) in te voeren als pre-Windows-referenties zijn ingeschreven. Wanneer u alle gebruikersgegevens wist, worden het ControlVault-beheerderswachtwoord en het systeemwachtwoord opnieuw ingesteld. Het ControlVault-beheerderswachtwoord kan alleen op deze manier worden gewist.

Opmerking: wanneer u alle gebruikersgegevens hebt gewist, wordt u gevraagd om uw computer opnieuw op te starten. Voor een goede werking van uw systeem is het belangrijk dat u de computer opnieuw opstart.

Als u slechts referenties voor één gebruiker wilt wissen, hoeft u het ControlVault-beheerderswachtwoord niet opnieuw in te stellen. Wanneer u op **Gebruikersgegevens wissen** (Clear user data) klikt, wordt u gevraagd om de gebruiker te selecteren waarvoor u de ControlVault-referenties wilt wissen. Wanneer u een gebruiker selecteert, wordt u gevraagd om het systeemwachtwoord in te voeren (alleen als pre-Windows-referenties zijn ingeschreven).

Opmerkingen:

- Als in een foutbericht wordt gemeld dat het ControlVault-beheerderswachtwoord niet kan worden gemaakt, archiveert u uw referenties, wist u alle gebruikersgegevens uit de ControlVault, start u de computer opnieuw op en probeert u het wachtwoord opnieuw te maken.
- Als in een foutbericht wordt gemeld dat referenties voor één gebruiker niet uit de ControlVault kunnen worden gewist, archiveert u uw referenties en wist u alle gebruikersgegevens en probeert u vervolgens de gegevens voor die ene gebruiker opnieuw te wissen.
- Als in een foutbericht wordt gemeld dat de referenties in de ControlVault niet kunnen worden gewist voor alle gebruikers, kunt u overwegen om het systeem opnieuw in te stellen. **Belangrijk:** bekijk het Help-onderwerp Systeem opnieuw instellen voordat u probeert om het systeem opnieuw in te stellen, aangezien hiermee ALLE beveiligingsgegevens voor gebruikers worden gewist.
- Als in een foutbericht wordt gemeld dat geen back-up kan worden gemaakt van de ControlVault- en TPM-gegevens, schakelt u de TPM in het systeem-BIOS uit. Hiertoe start u de computer opnieuw op, drukt u op de **F2**-toets wanneer de back-up wordt gestart, om toegang te krijgen tot de BIOS-instellingen en navigeert u vervolgens naar Security>TPM Security. Schakel de TPM vervolgens opnieuw in en probeer uw ControlVault-gegevens opnieuw te archiveren.
- Bezoek wave.com/support/Dell voor meer gedetailleerde informatie over een specifiek foutbericht.

Self-Encrypting Drives: geavanceerd

Dell Data Protection | Accessbeheert de hardwaregebaseerde beveiligingsfuncties van Self-Encrypting Drives, waarop gegevensversleuteling in de stationshardware is ingesloten. Dit beheer garandeert dat alle bevoegde gebruikers toegang krijgen tot versleutelde gegevens wanneer de stationsvergrendeling is ingeschakeld.

Het venster Self-Encrypting Drive in **Apparaatbeheer** (Device Management) wordt alleen weergegeven wanneer een of meer Self-Encrypting Drives (SED) aanwezig zijn in het systeem.

Belangrijk: wanneer het station is ingesteld, zijn Self-Encrypting Drive-gegevensbeveiliging en stationsvergrendeling "ingeschakeld".

Stationsbeheer
Met deze functies kan de stationsbeheerder instellingen voor de stationsbeveiliging beheren. Wijzigingen aan de instellingen voor de stationsbeveiliging treden in werking nadat het station is uitgeschakeld.

Gegevensbeveiliging
Hier wordt de status *Ingeschakeld* of *Uitgeschakeld* voor de Self-Encrypting Drive-gegevensbeveiliging weergegeven. De status Ingeschakeld houdt in dat de stationsbeveiliging is ingesteld. Totdat *stationsvergrendeling* is ingeschakeld, hoeven gebruikers zich niet te verifiëren bij pre-Windows-toegang tot het station.

Hier kunt u de Self-Encrypting Drive-gegevensbeveiliging inschakelen. Wanneer deze is uitgeschakeld, zijn alle geavanceerde beveiligingsfuncties van de Self-Encrypting Drive uitgeschakeld en fungeert het station als een standaardstation. Door de gegevensbeveiliging uit te schakelen, worden ook alle beveiligingsinstellingen verwijderd, waaronder de referenties van de stationsbeheerder en de stationsgebruikers. Deze functie verandert, noch verwijdert enige gebruikersgegevens op het station.

Vergrendeling
Hier wordt de status *Ingeschakeld* of *Uitgeschakeld* voor Self-Encrypting Drives weergegeven. Zie het onderwerp Self-Encrypting Drive voor informatie over de werking van een vergrendeld station.

Mogelijk dient u de stationsvergrendeling tijdelijk uit te schakelen. U kunt dit hier doen. Dit wordt echter niet aanbevolen omdat geen referenties vereist zijn om toegang te krijgen tot het station wanneer stationsvergrendeling is uitgeschakeld. Elke platformgebruiker kan dus toegang krijgen tot de stationsgegevens. Door de stationsvergrendeling uit te schakelen, wordengeen beveiligingsinstellingen verwijderd, ook niet de referenties van de stationsbeheerder en de stationsgebruikers, of eventuele gebruikersgegevens op het station.

Waarschuwing:als u de installatie van de toepassing **Dell Data Protection | Access** ongedaan maakt, moet u eerst de Self-Encrypting Drive-gegevensbeveiliging uitschakelen en het station ontgrendelen.

Stationsbeheerder

Hier wordt de huidige stationsbeheerder weergegeven. De stationsbeheerder kan hier wijzigen welke gebruiker de stationsbeheerder is. De nieuwe beheerder moet een geldige Windows-gebruiker met beheerdersbevoegdheden op het systeem zijn. Er kan slechts één stationsbeheerder op het systeem zijn.

Stationsgebruikers

Hier worden de ingeschreven stationsgebruikers weergegeven, alsook het aantal gebruikers dat momenteel is ingeschreven. Het maximum aantal gebruikers dat wordt ondersteund, is afhankelijk van de Self-Encrypting Drive (momenteel 4 gebruikers voor Seagate-stations en 24 voor Samsung-stations).

Windows Wachtwoordsynchronisatie

Met de functie Windows Wachtwoordsynchronisatie (WPS) worden de Self-Encrypting Drive-wachtwoorden automatisch ingesteld zodat deze identiek zijn aan uw Windows-wachtwoord. Deze functie wordt niet afgedwongen voor de stationsbeheerder, maar is alleen van toepassing op stationsgebruikers. De WPS-functionaliteit kan worden gebruikt in bedrijfsomgevingen waarin wachtwoorden na specifieke tijdsintervallen (bijvoorbeeld elke 90 dagen) worden gewijzigd. Als deze optie is ingeschakeld, worden de Self-Encrypting Drive-wachtwoorden voor alle gebruikers automatisch bijgewerkt wanneer deze Windows-wachtwoorden worden gewijzigd.

Opmerking: wanneer Windows Wachtwoordsynchronisatie is ingeschakeld, kan het Self-Encrypting Drive-wachtwoord van een gebruiker niet worden gewijzigd. Hun Windows-wachtwoord moet worden gewijzigd zodat het stationswachtwoord automatisch wordt bijgewerkt.

Laatste gebruikersnaam onthouden

Wanneer deze optie is ingeschakeld, wordt de laatst ingevoerde gebruikersnaam weergegeven in het veld **Gebruikersnaam** van het pre-Windows-verificatiescherm.

Gebruikersnaam selecteren

Wanneer deze optie is ingeschakeld, kunnen gebruikers alle gebruikersnamen voor het station in het veld **Gebruikersnaam** van het pre-Windows-verificatiescherm bekijken.

Cryptografisch wissen

Met deze optie kunt u alle gegevens op de Self-Encrypting Drive wissen. Hierdoor worden geen gegevens gewist, maar worden de sleutels verwijderd waarmee de gegevens worden versleuteld. Daarna zijn deze gegevens onbruikbaar. U kunt de stationsgegevens na cryptografisch wissen op geen enkele wijze terughalen. Bovendien is Self-Encrypting Drive-gegevensbeveiliging uitgeschakeld en het station is gereed om een nieuwe bestemming te krijgen.

Opmerkingen:

- Als fouten met de Self-Encrypting Drive-beheerfuncties optreden, schakelt u de computer eerst volledig uit (niet rechtstreeks opnieuw opstarten) voordat u deze vervolgens opnieuw opstart.
- Bezoek wave.com/support/Dell voor meer gedetailleerde informatie over een specifiek foutbericht.

Informatie over verificatieapparaat

Het venster Informatie over verificatieapparaat (Authentication Device Information) in **Apparaatbeheer** (Device Management) bevat informatie en een status voor alle aangesloten verificatieapparaten (bijvoorbeeld vingerafdruklezers, lezers voor traditionele of contactless smartcards) op het systeem.

Technische ondersteuning

Technische ondersteuning voor de **Dell Data Protection | Access**-software vindt u op http://www.wave.com/support.dell.com.

Wave TCG Enabled CSP

De Wave Systems Trusted Computing Group (TCG) enabled Cryptographic Service Provider (CSP) maakt deel uit van de toepassing **Dell Data Protection | Access** en is beschikbaar voor gebruik wanneer een CSP is vereist. De vereiste CSP kan rechtstreeks vanuit een toepassing worden aangeroepen of in een lijst met geïnstalleerde CSP's worden geselecteerd. Selecteer, indien mogelijk, de "Wave TCG Enabled CSP" om er zeker van te zijn dat de TPM de sleutels genereert en dat de sleutels en hun wachtwoorden door **Dell Data Protection | Access** worden beheerd.

Dankzij de Wave Systems TCG Enabled CSP kunnen toepassingen rechtstreeks via MSCAPI functies gebruiken die op TCG-compatibele platforms beschikbaar zijn. Op de TPM wordt een asymmetrische sleutelfunctionaliteit aangeboden door een TCG-Enhanced MSCAPI CSP-module, die ook gebruikmaakt van de verbeterde beveiliging die de TPM biedt, ongeacht leveranciersspecifieke vereisten voor de Trusted Software Stack (TSS)-provider.

Opmerking: als TPM-sleutels die door de Wave TCG enabled CSP zijn gegenereerd, een wachtwoord vereisen en de gebruiker een TPM-hoofdwachtwoord heeft gemaakt, worden de afzonderlijke sleutelwachtwoorden willekeurig gegenereerd en opgeslagen in de TPM-wachtwoordenkluis.