Dell adatvédelem | Elérés kezdőlap

A **Dell adatvédelem | Elérés** kezdőlap az alkalmazásfunkciók elérésének kiindulópontja. Ebben az ablakban a következőket érheti el:

Rendszerhozzáférés varázsló
Elérési lehetőségek
Self-Encrypting Drive
Haladó beállítások

Az ablak jobb alsó sarkában található egy **haladó** nevű hivatkozás, amelyre kattintva elérheti a haladó beállításokat.

A kezdőlapra való visszatéréshez a haladó beállítások ablakban kattintson a jobb alsó sarokban lévő **kezdőlap** hivatkozásra.

Rendszerhozzáférés varázsló

A Rendszerhozzáférés varázsló automatikusan elindul a **Dell adatvédelem | Elérés** alkalmazás első indításakor. Ez a varázsló végigvezeti a rendszer összes biztonsági szolgáltatásának beállításán, beleértve azt is, hogy a rendszerbe hogyan (pl. csak jelszóval vagy ujjlenyomattal és jelszóval együtt) és mikor (a Window és/vagy pre-Windows rendszerbe) kíván bejelentkezni. Emellett ha a rendszer self-encrypting drive egységgel rendelkezik, akkor azt is konfigurálni tudja ezzel a varázslóval.

Rendszergazda-funkciók

A rendszer Windows rendszergazdai jogosultságokkal ellátott felhasználói képesek elvégezni a **Dell adatelérés | Adatvédelem** következő funkcióit, amelyekre az általános jogú felhasználóknak nincs joguk:

- A rendszerjelszó (Pre-Windows) beállítása / módosítása
- A merevlemezjelszó beállítása / módosítása
- A rendszergazdai jelszó beállítása / módosítása
- A TPM tulajdonosi jelszó beállítása / módosítása
- A ControlVault rendszergazdai jelszó beállítása / módosítása
- Rendszer-visszaállítás
- Azonosítók archiválása és visszaállítása
- A smartcard rendszergazdai PIN-kódjának beállítása / módosítása
- Smartcard törlése / alaphelyzetbe állítása
- A Windowsba történő Dell biztonságos bejelentkezés engedélyezése / letiltása
- A Windows bejelentkezési házirend beállítása
- A self-encrypting drive egységek kezelése, pl.:
    - A self-encrypting drive egységek zárolásának engedélyezése / letiltása
    - A Windows jelszó-szinkronizálás (WPS) engedélyezése / letiltása
    - Single Sign On (SSO) engedélyezése / letiltása
    - Kriptografikus törlés végrehajtása

Távoli kezelés

Szervezete kialakíthat olyan környezetet, amelyben a több platformon megtalálható **Dell adatvédelem | Elérés** alkalmazás biztonsági funkcióinak kezelése központilag (azaz távoli kezeléssel) történik. Ebben az esetben a Windows biztonsági infrastruktúrája, például az Active Directory használható a **Dell adatvédelem | Elérés** adott funkcióinak biztonságos kezeléséhez.

A számítógépek távoli kezelése során (amikor pl. a távoli rendszergazda a „tulajdonos”), megtörténik a **Dell adatvédelem | Elérés** funkció helyi felügyeletének letiltása, így az alkalmazás kezelőablakai nem lesznek helyileg elérhetőek. A következő funkciók kezelése végezhető távolról:

- Trusted Platform Module (TPM)
- ControlVault
- Pre-Windows bejelentkezés
- Rendszer-visszaállítás
- BIOS jelszavak
- Windows bejelentkezési házirend
- Self-Encrypting Drive egységek
- Ujjlenyomat- és Smartcardbeolvasás

Ha a Wave Systems távoli kezelésre szolgáló EMBASSY® Távoli felügyeleti kiszolgáló (ERAS) termékével kapcsolatban bővebb információkra van szüksége, akkor lépjen kapcsolatba Dell kereskedőjével, vagy látogasson el a dell.com oldalra.

Elérési lehetőségek

Az Elérési lehetőségek ablakban beállíthatja, hogyan kíván hozzáférni rendszeréhez.

Ha vannak beállított **Dell Adatvédelem | Elérés** lehetőségek, ezek meg fognak jelenni a kezdőlapon az elérhető beállításokkal (pl. jelszó módosítása a Pre-Windows bejelentkezéshez). Az elérhető beállítások parancsikonok, amelyekre ha rákattint, egy adott feladatot végző megfelelő ablakhoz viszik (pl. a pre-Windows jelszó módosítása vagy egy másik ujjlenyomat beolvasása).

Általános
Először megadhatja a bejelentkezés időpontját (Windows, pre-Windows vagy mindkettő) és módját (pl. ujjlenyomattal vagy jelszóval). A bejelentkezés módját illetően egy vagy két lehetőség közül választhat, amelyek az ujjlenyomattal, smartcarddal és jelszóval történő bejelentkezések kombinációit tartalmazzák. A felsorolt lehetőségek a környezetében alkalmazott bejelentkezési házirendeken és a platform által támogatott módokon alapulnak.

Ujjlenyomat
Ha rendszere tartalmaz ujjlenyomat-olvasót, beolvashatja vagy frissítheti a rendszerbe való bejelentkezéshez használt ujjlenyomatokat. Miután beolvasta az ujjlenyomatokat, lehúzhatja a beolvasott ujja(ka)t a rendszer ujjlenyomat-leolvasóján a Windows, pre-Windows vagy mindét platformon működő rendszerének eléréséhez (attól függően, hogy mit adott meg az Általános elérési lehetőségekben). Bővebb tájékoztatás a Felhasználói ujjlenyomatok beolvasása című szakaszban található.

Pre-Windows bejelentkezés
Ha azt adta meg, hogy a felhasználóknak a pre-Windows rendszerbe kell bejelentkezniük, akkor a pre-Windows eléréshez be kell állítania egy rendszerjelszót (melyet időnként pre-Windows jelszónak is szokás nevezni) . Ha ez be van állítva, a rendszergazda bármikor módosíthatja a jelszót.

Ezen a képernyőn le is tilthatja a pre-Windows bejelentkezést: ehhez írja be az aktuális rendszerjelszavát, ellenőrizze a jelszó helyességét, majd kattintson a **Letiltás** gombra.

Smartcard
Ha azt adta meg, hogy a felhasználóknak smartcard bejelentkezést kell használniuk, akkor be kell olvasnia egy vagy több hagyományos (contacted) vagy contactless smartcardot. Kattintson a **Másik smartcard beolvasása** hivatkozásra a smartcard beolvasás varázsló elindításához. A beolvasás a smartcard bejelentkezéshez történő felhasználásának beállítását jelenti.

Miután beolvasott egy smartcardot, a kártya PIN-kódját a **Saját smartcard PIN-kód módosítása vagy beállítása** hivatkozás segítségével módosíthatja vagy állíthatja be.

Pre-Windows bejelentkezés

A pre-Windows bejelentkezés beállítása esetén gondoskodnia kell a rendszer bekapcsolásakor, a Windows betöltése előtt (jelszó, ujjlenyomat vagy smartcard segítségével) végzett azonosításról. A pre-Windows bejelentkezési funkció további biztonságot kínál a rendszer számára, meggátolva az illetéktelen felhasználókat a Windows veszélyeztetésében és a számítógéphez való hozzáférésben (pl. számítógéplopás esetén).

A Pre-Windows bejelentkezési ablakban a rendszergazdák beállíthatják a pre-Windows bejelentkezést, létrehozhatnak vagy módosíthatnak egy pre-Windows jelszót (rendszerjelszót), ha pedig már megtörtént ennek a jelszónak a létrehozása, akkor ebben az ablakban letilthatják a pre-Windows bejelentkezést. A pre-Windows bejelentkezés beállítása elindít egy varázslót, amely a következőket hajtja végre:

- Rendszerjelszó: Beállít egy rendszerjelszót (más néven pre-Windows jelszót) a pre-Windows elérés számára. Ez a jelszó biztonsági jelszóként is szolgál olyan esetekben, amikor egy felhasználó további hitelesítési lehetőségekkel rendelkezik (pl. képes elérni a rendszert, ha probléma lép fel az ujjlenyomat-leolvasóval).
- Ujjlenyomat vagy Smartcard: Beállít egy ujjlenyomatot vagy egy smartcard eszközt a pre-Windows bejelentkezés során történő használatra, és megadja, hogy ez a hitelesítési lehetőség a pre-Windows jelszó mellett, vagy azt helyettesítve kerül-e felhasználásra.
- Single Sign On: Alapértelmezés szerint a pre-Windows azonosítás (jelszó, ujjlenyomat vagy smartcard) szolgál a Windowsba való automatikus bejelentkezésre is (ezt szokás „Single Sign On” bejelentkezésnek nevezni). Ennek a funkciónak a letiltásához jelölje be az „Újra be szeretnék jelentkezni a Windowsban” jelölőnégyzetet.
- Ha a pre-Windows jelszó mellett egy BIOS merevlemezjelszó is beállításra került, akkor lehetősége lesz a merevlemezjelszó megváltoztatására vagy letiltására is.

MEGJEGYZÉS: Nem minden ujjlenyomat-leolvasó engedélyezett a pre-Windows bejelentkezéssel történő használat céljából. Ha olvasója nem kompatibilis, akkor csak a Windows-bejelentkezéshez tud ujjlenyomatokat beolvasni. Az adott ujjlenyomat-leolvasó kompatibilitásának megállapítása érdekében forduljon a rendszergazdához, vagy látogasson el a support.dell.com oldalra a támogatott ujjlenyomat-leolvasók listájának megtekintéséhez.

Pre-Windows bejelentkezés letiltása
Ebben az ablakban is letilthatja a pre-Windows bejelentkezést: ehhez írja be az aktuális pre-Windows jelszavát (rendszer-jelszavát), ellenőrizze a jelszó helyességét, majd kattintson a **Letiltás** gombra. Ne feledje, hogy a pre-Windows bejelentkezés letiltásakor a beolvasott ujjlenyomatok vagy smartcard eszközök beolvasott állapotban maradnak.

Ujjlenyomatok beolvasása

A felhasználók regisztrálhatják vagy frissíthetik az ujjlenyomatokat, amelyek a rendszer számára történő azonosításra használhatók a pre-Windows vagy Windows rendszerbeli bejelentkezés során. Ha vannak beolvasott ujjlenyomatok, akkor az Ujjlenyomat lapon elhelyezett, kezeket ábrázoló képeken látható, hogy azok mely ujjakról készültek. A **Másik beolvasása** hivatkozásra kattintva elindíthatja az Ujjlenyomat beolvasása varázslót, amely végigvezeti a beolvasás folyamatán. A „Beolvasás" egy ujjlenyomat mentését jelenti a bejelentkezéshez való felhasználás céljából. Az ujjlenyomatok beolvasásához megfelelően telepített és konfigurált, érvényes ujjlenyomat-leolvasóval kell rendelkeznie.

MEGJEGYZÉS: Nem minden ujjlenyomat-leolvasó használható pre-Windows bejelentkezéshez. Hibaüzenet jelenik meg, ha nem kompatibilis ujjlenyomat-leolvasóval próbál beolvasást végezni a pre-Windows rendszer számára. Az eszközök kompatibilitásának megállapítása érdekében forduljon a rendszergazdához, vagy látogasson el a support.dell.com oldalra a támogatott ujjlenyomat-leolvasók listájának megtekintéséhez.

Ujjlenyomatok beolvasásakor személyazonosságának igazolása céljából be kell írnia Windows-jelszavát. Ha házirendje megköveteli, a rendszer felszólítására a Pre-Windows jelszót (rendszerjelszót) is be kell írnia. A Pre-Windows jelszó igénybe vehető a rendszerhez való hozzáféréshez, ha probléma merült fel az ujjlenyomat-leolvasóval.

MEGJEGYZÉSEK:

- A beolvasás során érdemes legalább két ujjlenyomatot beolvastatnia.
- Ügyeljen arra, hogy a rendszer megfelelően rögzítse az ujjlenyomatait, mielőtt engedélyezi az ujjlenyomat alapú azonosítást.
- Ha ujjlenyomat-leolvasót cserél egy rendszerben, akkor az új ujjlenyomat-leolvasóval ismét be kell olvasnia az ujjlenyomatokat. A két különböző ujjlenyomat-leolvasó közötti váltogatás nem ajánlott.
- Ha ismétlődő „az érzékelő elveszítette a fókuszt" üzeneteket lát az ujjlenyomatok beolvasásakor, ez lehet, hogy azt jelenti, hogy a számítógép nem ismeri fel az ujjlenyomat-leolvasót. Ha külső ujjlenyomat-leolvasót használ, az olvasó leválasztása, majd újbóli csatlakoztatása gyakran megoldást jelent a problémára.

Beolvasott ujjlenyomatok törlése
Lehetősége van eltávolítani a beolvasott ujjlenyomatokat: kattintson az **Ujjlenyomat eltávolítása** hivatkozásra vagy egy beolvasott ujjlenyomatra (a kiválasztás megszüntetéséhez) az Ujjlenyomat beolvasása varázslóban.

Az adott, beolvasott ujjlenyomatokkal rendelkező felhasználó pre-Windows azonosításból való eltávolításához a rendszergazda megszüntetheti a felhasználó összes beolvasott ujjlenyomatának kiválasztását.

MEGJEGYZÉS: Ha az ujjlenyomat-beolvasási folyamat során hibát tapasztal, a wave.com/support/Dell oldalon találhat további információkat.

Smartcard beolvasása

A **Dell adatvédelem | Elérés** lehetőséget ad hagyományos (contacted) vagy contactless Smartcard kártya használatára a saját Windows fiókba való bejelentkezéshez vagy a pre-Windows hitelesítéshez. A Smartcard lapon kattintson a **Másik smartcard beolvasása** hivatkozásra a Smartcard beolvasás varázsló elindításához, amely végigvezeti a beolvasási folyamaton. A „beolvasás" a smartcard bejelentkezéshez történő felhasználásának beállítását jelenti.

A beolvasás végrehajtásához megfelelően telepített és konfigurált, érvényes smartcard azonosító eszközzel kell rendelkeznie.

MEGJEGYZÉS: Az adott eszközök kompatibilitásának megállapítása érdekében forduljon a rendszergazdához, vagy látogasson el a support.dell.com oldalra a támogatott smartcard eszközök listájának megtekintéséhez.

Beolvasás
Smartcard beolvasásakor személyazonosságának igazolása céljából be kell írnia Windows-jelszavát. Ha házirendje megköveteli, a rendszer felszólítására a Pre-Windows jelszót (rendszerjelszót) is be kell írnia. A Pre-Windows jelszó igénybe vehető a rendszerhez való hozzáféréshez, ha probléma merült fel a smartcard olvasóval.

Beolvasás közben be kell írnia a smartcard PIN-kódját, ha az beállításra került. Ha házirendje megköveteli a PIN-kódot, és az még nem került beállításra, akkor a rendszer felszólítására létre kell hoznia egyet.

MEGJEGYZÉSEK:

- Ha egy felhasználó smartcard használatra van beállítva a pre-Windows rendszerben, akkor a felhasználót nem lehet eltávolítani.
- Míg az általános jogú felhasználók a felhasználói PIN-kódot módosíthatják a smartcard eszközön, addig a rendszergazda mind a rendszergazdai PIN-kódot, mind a felhasználói PIN-kódot megváltoztathatja.
- A rendszergazda alaphelyzetbe is állíthatja a smartcard kártyát. Az alaphelyzetbe állítás után a smartcard addig nem használható a Windows rendszerbe való bejelentkezés hitelesítése vagy a pre-Windows rendszer esetén, amíg nem történt meg az újbóli beolvasása.

MEGJEGYZÉS: A TPM tanúsítvány hitelesítéséhez a rendszergazdák a Microsoft Windows smartcard beolvasási folyamatán keresztül beolvashatják a TPM tanúsítványokat. Az alkalmazással való kompatibilitás érdekében a rendszergazdáknak a Smartcard CSP helyett a „Wave TCG-Enabled CSP" funkciót kell Kriptográfiai szolgáltatóként kiválasztaniuk. Emellett a megfelelő felhasználóazonosítási házirend beállításával engedélyezni kell az ügyfél számára a Dell biztonságos bejelentkezést.

MEGJEGYZÉS: Ha hibaüzenetet kap arról, hogy nem fut a Smartcard szolgáltatás, a következő módon elindíthatja / újraindíthatja ezt a szolgáltatást:

- Navigáljon a Vezérlőpultról a Felügyeleti eszközök ablakba, válassza ki a Szolgáltatás elemet, majd kattintson a jobb egérgombbal a Smartcard lehetőségre, és válassza ki a helyi menü Indítás vagy Újraindítás menüpontját.
- Egy megadott hibaüzenettel kapcsolatban további információkért keresse fel a wave.com/support/Dell oldalt.

Self-Encrypting Drive áttekintés

A **Dell adatvédelem | Elérés** kezeli a self-encrypting drive egységek hardver alapú biztonsági funkcióit, amelyek beépített titkosítással rendelkeznek a meghajtó hardverében. Ez a funkció biztosítja, hogy a titkosított adatokhoz kizárólag a jogosult felhasználók férhessenek hozzá (ha a meghajtó zárolása engedélyezve van).

A Self-Encrypting Drive ablak az alul lévő **Self-Encrypting Drive** lapra való kattintással érhető el. Ez a lap csak akkor jelenik meg, amikor egy vagy több self-encrypting drive egység (SED) található a rendszerben.

Kattintson a **Beállítás** hivatkozásra a Self-Encrypting Drive beállító varázsló elindításához. Ebben a varázslóban létre fog hozni egy Meghajtó-rendszergazdai jelszót, biztonsági másolatot készít róla, és alkalmazza a meghajtó titkosítási beállításait. Csak a rendszergazdák érhetik el a Self-Encrypting Drive beállító varázslót.

Fontos! Miután megtörtént a meghajtó beállítása, „engedélyezve” van az adatvédelem és a meghajtó zárolása. A meghajtó zárolt állapotában a következő módon viselkedik:

- A meghajtó belép a *zárolt* üzemmódba, amikor megtörténik a meghajtó áramellátásának kikapcsolása.
- A meghajtó nem indul el, hacsak a felhasználó be nem írja a helyes felhasználónevet és jelszót (vagy megadja ujjlenyomatát) a Pre-Windows bejelentkező képernyőn. A meghajtó zárolt állapotának engedélyezése előtt a meghajtón lévő adatok a számítógép bármely felhasználója számára elérhetők.
- A meghajtó még akkor is védve van, ha azt egy másik számítógéphez másodlagos meghajtóként csatlakoztatják; hitelesítés szükséges a meghajtón lévő adatok eléréséhez.

Miután megtörtént a meghajtó beállítása, a Self-Encrypting Drive ablak megjeleníti a meghajtó(ka)t és egy hivatkozást a felhasználók számára meghajtójelszavuk megváltoztatásához. Ha Ön meghajtó-rendszergazda, akkor ebben az ablakban képes lesz elvégezni a meghajtófelhasználók hozzáadását vagy eltávolítását. Ha van beállított külső meghajtó, akkor az meg fog jelenni ebben az ablakban, és meg lehet szüntetni a zárolását.

MEGJEGYZÉS: Egy másodlagos, külső meghajtó zárolásához a meghajtót a számítógéptől függetlenül ki kell kapcsolni.

A meghajtó beállításait a meghajtó-rendszergazda kezelheti a **Haladó>Eszközök** pontban. Bővebb információkért lásd az Eszközkezelés – Self-Encrypting Drive egységek című részt.

Meghajtóbeállítás

A Self-Encrypting Drive beállító varázsló végigvezeti a meghajtó(k) beállításának folyamatán. A következő fogalmakat fontos szem előtt tartani, miközben végighalad ezen a folyamaton.

Meghajtó-rendszergazda
A meghajtó elérését beállító első, rendszergazdai jogosultsággal rendelkező felhasználó (aki beállítja a meghajtó rendszergazdai jelszavát) lesz a meghajtó-rendszergazda; csak ez a felhasználó rendelkezik a meghajtó elérésének megváltoztatásához szükséges jogosultságokkal. Annak megerősítése érdekében, hogy az első felhasználó szándékosan lett a meghajtó rendszergazda, be kell jelölnie a „Megértettem” jelölőnégyzetet, ha tovább kíván haladni ezzel a lépéssel.

Meghajtó-rendszergazdai jelszó
A varázsló megkéri a meghajtó-rendszergazdai jelszó létrehozására, és megerősítés céljából a jelszó újbóli beírására. Be kell írnia Windows-jelszavát személyazonosságának igazolására,

mielőtt létrehozhatná a meghajtó-rendszergazdai jelszavát. Az aktuális Windows felhasználónak rendszergazdai jogosultságokkal kell rendelkeznie ennek a jelszónak a létrehozásához.

A meghajtó azonosítóinak biztonsági mentése
A meghajtó-rendszergazdai azonosítók biztonsági másolatának mentéséhez írjon be egy helyet, vagy egy hely kiválasztásához kattintson a **Tallózás** gombra.

FONTOS**!**

- Erősen javasolt biztonsági másolatot készíteni ezekről az azonosítókról, és az elsődleges merevlemeztől eltérő meghajtóra (pl. cserélhető adathordozóra) menteni őket. Ellenkező esetben ha elveszíti az elérését a meghajtóhoz, a biztonsági mentéshez sem fog tudni hozzáférni.
- Miután befejezte a meghajtó beállítását, mindenfelhasználónak be kell majd írnia a helyes felhasználónevet és jelszót (vagy meg kell adnia ujjlenyomatát), mielőtt a Windows betöltődik, hogy hozzáférjen a rendszerhez annak legközelebbi bekapcsolásakor.

Meghajtófelhasználó hozzáadása
A meghajtó-rendszergazda hozzáadhat más, érvényes Windows felhasználókat a meghajtóhoz. A felhasználók meghajtóhoz való hozzáadásakor a rendszergazdának lehetősége van kérni a jelszó visszaállítását az első bejelentkezés alkalmával. A meghajtó zárolásának megszüntetéséhez a felhasználónak vissza kell állítania jelszavát a pre-Windows hitelesítő képernyőn.

Haladó beállítások

- *Single Sign On* – Alapértelmezés szerint a Windowsba való automatikus bejelentkezés is a pre-Windows rendszerben a meghajtón történő azonosítás céljából beírt Self-Encrypting Drive jelszóval történik (ezt szokás „Single Sign On” bejelentkezések nevezni). Ennek a funkciónak a letiltásához a meghajtó beállításainak konfigurálásakor jelölje be az „Újra be szeretnék jelentkezni a Windows indításakor” jelölőnégyzetet.
- *Ujjlenyomatos bejelentkezés* – A támogatott platformokon meghatározhatja, hogy a self-encrypting drive egységen a jelszava helyett az ujjlenyomatával szeretné magát azonosítani.
- *Alvó/készenléti (S3) támogatás* (ha a platform támogatja) – Ha engedélyezve van, self-encrypting drive egysége biztonságosan alvó/készenléti üzemmódba (más néven S3 üzemmódba) helyezhető, és pre-Windows azonosítást kér az alvó/készenléti üzemmódból való visszatéréskor.

MEGJEGYZÉSEK:

- Amikor engedélyezve van az S3 támogatás, a meghajtó titkosítási jelszavai a BIOS jelszó esetleges korlátozásainak tárgyát képezhetik. A BIOS jelszóra érvényes esetleges rendszerbeli korlátozásokról a rendszerhardver gyártója adhat bővebb tájékoztatást.
- Nem minden self-encrypting drive támogatja az S3 üzemmódot. A meghajtó beállítása közben értesítést kap arról, hogy a meghajtó támogatja-e a készenléti/alvó üzemmódot. Azoknál a meghajtóknál, amelyek nem támogatják ezt az üzemmódot, a Windows S3 kérések automatikusan hibernálási kérésekké kerülnek átalakításra, ha a hibernálás üzemmód engedélyezve van (a számítógépen erősen javasolt a hibernálás üzemmód engedélyezése).
- A Single Sign On (SSO) beállítását követő első bejelentkezésekor a folyamat megáll a Windows bejelentkezési képernyőnél. Meg kell adnia Windows-hitelesítése módját, és a program ezt biztonságosan eltárolja a jövőbeli Windows-bejelentkezésekhez. A következő rendszerindítás alkalmával az SSO automatikusan bejelentkezteti a Windows rendszerbe. Ugyanerre a folyamatra van szükség akkor is, amikor egy felhasználó Windows-hitelesítése (jelszava, ujjlenyomata, Smartcard PIN-kódja) megváltozik. Ha a számítógép egy tartományban található, és a tartomány házirendje megköveteli a

ctrl+alt+del billentyűkombináció megnyomását a Windowsba való bejelentkezéskor, a rendszer tiszteletben tartja majd ezt a házirendet.

VIGYÁZAT! Ha eltávolítja a **Dell adatvédelem | Elérés** alkalmazást, először le kell tiltania a self-encrypting drive adatvédelmet, és meg kell szüntetnie a meghajtó zárolását.

SED felhasználói funkciók

A self-encrypting drive rendszergazdák elvégezhetik a meghajtóbiztonság és a felhasználók kezelésével kapcsolatos összes feladatot. Azok a meghajtófelhasználók, akik nem a meghajtó rendszergazdái, csak a következő feladatokat képesek elvégezni:

- Saját meghajtójelszó módosítása
- Meghajtó zárolásának feloldása

Ezek a feladatok a **Dell adatvédelem | ElérésSelf-Encrypting Drive** lapján érhetők el.

Jelszó módosítása
A beolvasott felhasználók létrehozhatják új meghajtóhitelesítési jelszavukat. A meghajtójelszó új értékének beállítása előtt be kell írnia az aktuális Self-Encrypting Drive jelszót.

MEGJEGYZÉSEK:

- Ha engedélyezve vannak, akkor az alkalmazás ellenőrzi a Windows-jelszavak hosszára és bonyolultságára vonatkozó házirendek betartását. Ha a Windows-jelszavakra vonatkozó házirend nincs engedélyezve, akkor a Self-Encrypting Drive jelszó hossza legfeljebb 32 karakter lehet. Ne feledje, hogy a maximális hossz 127 karakter, ha az S3 (készenlét/alvás) nincs engedélyezve.
- A felhasználó Self-Encrypting Drive jelszava eltér Windows-jelszavától. Amikor a felhasználó módosítja vagy visszaállítja Windows-jelszavát, meghajtójelszava változatlan marad, kivéve akkor, ha engedélyezve van a Windows jelszó-szinkronizálás. Bővebb információk az Eszközök: Self-Encrypting Drive egységek részben találhatók.
- Néhány nem angol nyelvű billentyűzeten találhatók olyan tiltott karakterek, amelyek a self-encrypting drive jelszavában nem használhatók. Ha a tiltott karakterek közül bármelyik szerepel a Windows-jelszóban, és engedélyezve van a Windows jelszó-szinkronizálás, akkor a szinkronizálás sikertelen lesz, és hibaüzenet jelenik meg.

Meghajtó zárolásának feloldása
A meghajtó zárolásának feloldása lehetővé teszi egy beolvasott meghajtófelhasználó számára egy zárolt meghajtó zárolásának feloldását. Ha a meghajtó zárolása engedélyezve van, akkor a meghajtó a számítógép kikapcsolása után mindig zárolt állapotba lép. A rendszer újbóli bekapcsolásakor a jelszó pre-Windows azonosító képernyőn történő beírásával azonosítania kell magát a meghajtón.

MEGJEGYZÉSEK:

- Előfordulhat, hogy nem lehet belépni az energiatakarékos üzemmódba (vagyis az alvó/készenléti vagy hibernált módba), ha egyszerre több self-encrypting drive felhasználói fiók is aktív a számítógépen.
- A pre-Windows azonosító képernyőn „User 1”, „User 2” stb. áll a meghajtó felhasználójának neve helyén az alkalmazás olyan verzióinál, amelyeknél a felhasználói felület nyelve a következők egyike: kínai, japán, koreai vagy orosz.

Haladó beállítások

A **Dell adatvédelem | Elérés** Haladó beállítások elemei lehetővé teszik a rendszergazdai jogosultságokkal rendelkező felhasználók számára az alkalmazás következő szolgáltatásainak kezelését:

Karbantartás
Jelszavak
Eszközök

MEGJEGYZÉS: Kizárólag a rendszergazdai jogosultságokkal rendelkező felhasználók végezhetnek módosításokat a Haladó beállítások elemeiben; az általános jogú felhasználók megtekinthetik ugyan ezeket a beállításokat, de nem hajthatnak végre változtatásokat.

Karbantartás áttekintése

A Karbantartás ablak segítségével a rendszergazdák megadhatják a Windows bejelentkezési beállításait, visszaállíthatják a rendszert más célból való felhasználásra, illetve archiválhatják vagy visszaállíthatják a rendszer biztonsági hardvere által tárolt felhasználói azonosítókat. A részletekért tekintse meg a következő témaköröket:

Elérési beállítások
Rendszer-visszaállítás
Azonosítók archiválása & visszaállítása

Elérési beállítások

Az Elérési beállítások ablak a rendszergazdák számára a Windows-bejelentkezés beállításainak megadását teszi lehetővé a rendszer összes felhasználója számára.

A Dell biztonságos bejelentkezés engedélyezése
A szokásos Windows ctrl-alt-delete képernyő helyettesítésének lehetősége különböző hitelesítési eszközök használatára ad módot a Windows jelszó helyett (vagy mellett) a Windows eléréséhez. A hitelesítés második eszközeként választhatja egy ujjlenyomat hozzáadását is a Windows bejelentkezési folyamat biztonságosságának növelése érdekében. További hitelesítési eszközök, például smartcard vagy TPM tanúsítvány is hozzáadható a Windowsba való bejelentkezéshez.

MEGJEGYZÉSEK:

- A Dell biztonságos bejelentkezés engedélyezése a rendszer összes felhasználóját érinti.
- Javasolt ezt a beállítást AZUTÁN engedélyezni, miután a felhasználók beolvasták az ujjlenyomataikat vagy smartcardjukat.
- A beállítás engedélyezését követő első bejelentkezés alkalmával a szokásos házirend szerint kell hitelesítenie magát a Windows számára, majd a következő rendszerindítás során kell alkalmaznia az új hitelesítési eszköz(öke)t.

A Dell biztonságos bejelentkezés letiltása
Ez a beállítás letiltja a **Dell adatvédelem | Elérés** összes funkcióját a Windowsba való bejelentkezéshez. Ennek kiválasztása után újra a szokásos Windows bejelentkezési házirend lesz érvényes.

MEGJEGYZÉSEK:

- Ha a bejelentkezésre tett kísérlet során hibajelzést kap a biztonságos Windows-bejelentkezéssel kapcsolatban, tiltsa le, majd engedélyezze újra a Dell biztonságos bejelentkezés beállítást.
- Egy megadott hibaüzenettel kapcsolatban további információkért keresse fel a wave.com/support/Dell oldalt.

Rendszer-visszaállítás

A rendszer-visszaállítási funkció az összes felhasználói adat törlésére szolgál a platformon lévő valamennyi biztonsági hardverről, mely például egy számítógép más célra történő átállításához vehető igénybe. Ez a beállítás törli a rendszerben lévő összes jelszót, kivéve a Windows felhasználói jelszavakat, valamint a hardvereszközökön (pl. ControlVault és TPM egységen, illetve ujjlenyomat-leolvasókon) lévő adatokat. Self-encrypting drive egységek esetén ez a funkció az adatvédelmet is letiltja, így a meghajtó adatai elérhetővé válnak.

Meg kell erősítenie: tisztában van azzal, hogy a rendszer visszaállítását végzi, majd kattintson a **Következő** gombra. A rendszer visszaállításához a jelszót mindegyik biztonsági eszköz számára be kell írnia, ha azok korábban beállításra kerültek:

- TPM tulajdonosi
- ControlVault rendszergazdai
- BIOS rendszergazdai
- BIOS rendszer (pre-Windows)
- Merevlemez (BIOS)
- Self-Encrypting Drive rendszergazdai

MEGJEGYZÉS: A self-encrypting drive egységek esetén csak a meghajtó-rendszergazdai jelszó megadása szükséges, nem kell megadni az összes meghajtófelhasználó jelszavát.

Fontos! A rendszer visszaállításakor a törölt adatok helyreállításának egyetlen módja a korábban mentett archívumból történő visszaállítás. Ha nem rendelkezik ilyen archívummal, az adatokat nem lehet helyreállítani. Self-encrypting drive egység esetén csak a beállítási adatok törlődnek, a meghajtón tárolt személyes adatok nem.

Azonosítók archiválása & visszaállítása

Az Azonosítók archiválása és visszaállítása funkció a ControlVault és Trusted Platform Module (TPM) által tárolt valamennyi felhasználói azonosító (bejelentkezési és titkosítási információ) archiválására és visszaállítására szolgál. Ezen adatok biztonsági mentése fontos a számítógép újbóli jogosultságkiosztásához, vagy hardverhiba esetén az adatok visszaállításához. Ebben az esetben egy mentett archív fájlból egyszerűen visszaállíthatja az összes azonosítót az új számítógépen.

Az azonosítók archiválását és visszaállítását egyetlen felhasználó vagy a rendszer összes felhasználója számára is választhatja.

A felhasználói azonosítók a pre-Windows rendszerben használt adatokból, például beolvasott ujjlenyomat- és smartcardadatokból, valamint a TPM-ben tárolt kulcsokból állnak. A TPM a biztonsági alkalmazások igényei szerint létrehozza a kulcsokat, például egy digitális tanúsítvány előállítása kulcsokat hoz létre a TPM-ben.

MEGJEGYZÉS: Annak meghatározásához, hogy a TPM kulcsok archiválhatók-e a **Dell adatvédelem | Elérés** segítségével, tekintse meg a biztonsági alkalmazás dokumentációját. Általában a kulcsok előállításához „Wave TCG-Enabled CSP” funkciót használó alkalmazások támogatottak.

Azonosítók archiválása
Az azonosítók archiválásához tegye a következőket:

- Adja meg, hogy az azonosítók archiválását saját maga, vagy a rendszer összes felhasználója számára végzi-e.
- A rendszerjelszó (pre-Windows jelszó), ControlVault rendszergazdai jelszó és a TPM tulajdonosi jelszó megadásával biztosítsa az azonosítást a biztonsági hardver számára.
- Hozzon létre egy azonosítómentési jelszót.
- A **Tallózás** gombbal adjon meg egy archiválási helyet. Az archiválás helyeként egy cserélhető adathordozót, például USB flash meghajtót vagy egy hálózati meghajtót kell megadni, hogy az adatok a merevlemez meghibásodása esetén is védve legyenek.

Fontos megjegyzések:
- Jegyezze fel az archiválás helyét, mert a felhasználónak szüksége lesz erre az azonosítói információk visszaállításához.
- Jegyezze fel az azonosítómentési jelszót az adatok visszaállíthatóságának biztosítása érdekében. Ez azért fontos, mert ezt a jelszót nem lehet visszaállítani.
- Ha nem ismeri a TPM tulajdonosi jelszót, forduljon a rendszergazdához, vagy olvassa el a számítógéphez tartozó TPM beállítási utasításait.

Azonosítók visszaállítása
Az azonosítók visszaállításához tegye a következőket:

- Adja meg, hogy az azonosítók visszaállítását saját maga, vagy a rendszer összes felhasználója számára végzi-e.
- Tallózással keresse meg az archiválás helyét, és válassza ki az archív fájlt.
- Írja be az archiválás beállításakor létrehozott azonosítómentési jelszót.
- A rendszerjelszó (pre-Windows jelszó), ControlVault rendszergazdai jelszó és a TPM tulajdonosi jelszó megadásával biztosítsa az azonosítást a biztonsági hardver számára.

MEGJEGYZÉSEK:

- Ha az azonosító sikertelen visszaállításáról kap hibaüzenetet, és már többször próbálkozott a visszaállítás végrehajtásával, próbálja meg végrehajtani egy másik archív fájl visszaállítását. Ha ez sikertelen, hozzon létre egy másik azonosítóarchívumot, és próbálja meg a visszaállítást az új archívumból.
- Ha hibaüzenetet kap arról, hogy nem lehetett visszaállítani a TPM kulcsokat, hozzon létre egy azonosítóarchívumot, majd törölje a TPM-et a BIOS-ban. A TPM törléséhez indítsa újra a számítógépet, az archiválás kezdetekor nyomja meg az **F2** billentyűt a BIOS beállítások eléréséhez, majd navigáljon a Biztonság>TPM biztonság helyre. Ezután állítsa vissza a TPM tulajdonjogát, és próbálja meg újra az azonosítók visszaállítását.
- Egy megadott hibaüzenettel kapcsolatban további információkért keresse fel a wave.com/support/Dell oldalt.

Jelszókezelés

A Jelszókezelés ablakban a rendszergazda létrehozhatja vagy módosíthatja a rendszerben lévő összes biztonsági jelszót:

- Rendszer (más néven Pre-Windows)*
- Rendszergazdai*
- Merevlemez*
- ControlVault
- TPM tulajdonosi
- TPM mester
- TPM jelszótároló
- Self-Encrypting Drive

MEGJEGYZÉSEK:

- Csak az aktuális platformkonfigurációhoz használható jelszavak jelennek meg, így ez az ablak a rendszer konfigurációjától és állapotától függően változik.
- Azon fenti jelszavak, melyek mellett * látható, BIOS jelszavak, így a rendszer BIOS-án keresztül is módosíthatók.
- Nem hozhatók létre, illetve nem módosíthatók BIOS szintű jelszavak, ha a BIOS rendszergazda letiltotta a jelszavak módosítását.
- Egy self-encrypting drive **beállítás** hivatkozására kattintva elindul a Self-Encrypting Drive beállító varázsló; a **kezelés** lehetőségre kattintva pedig a felhasználó elvégezheti egy vagy több Self-Encrypting Drive jelszavának módosítását.
- Ha a **kezelés** hivatkozásra kattint a TPM jelszótároló esetében, akkor megjelenik egy ablak, amelyben megtekintheti vagy módosíthatja a TPM kulcsait védő jelszavakat. Ha létrejön egy jelszót igénylő TPM kulcs, a jelszó véletlenszerűen kerül előállításra és elhelyezésre a jelszótárolóban. Addig nem kezelheti a TPM jelszótárolót, amíg nem hozott létre egy TPM mesterjelszót.

Windows-jelszavak bonyolultsági szabályai

A **Dell adatvédelem| Elérés** biztosítja, hogy a következő jelszó megfelel a Windows jelszavakra vonatkozó bonyolultsági szabályainak:

- TPM tulajdonosi jelszó

A számítógépen a következőképpen tudja ellenőrizni a Windows-jelszavak bonyolultságára vonatkozó házirendet:

1. Nyissa meg a Vezérlőpultot.
2. Kattintson kétszer a Felügyeleti eszközök ikonra.
3. Kattintson kétszer a Helyi biztonsági házirend ikonra.
4. Bontsa ki a Fiókházirendek elemet, majd válassza a Jelszóházirend beállítást.

Eszközök áttekintése

Az Eszközök ablakot a rendszergazdák használják a rendszerben telepített összes biztonsági eszköz kezeléséhez. Minden eszköznél megtekintheti az eszköz állapotát és a kiegészítő, részletes információkat, például a firmware verzióját. Az egyes eszközökkel kapcsolatos információk megtekintéséhez kattintson a **megjelenítés** lehetőségre, vagy válassza az **elrejtés** elemet az adott szakasz összehúzásához. A kezelhető eszközök a platform tartalmától függően a következők:

Trusted Platform Module (TPM)
ControlVault®
Self-Encrypting Drive meghajtóegység(ek)
Azonosítóeszköz-információk

Trusted Platform Module (TPM)

A TPM biztonsági chipet engedélyezni kell, és létre kell hozni a TPM tulajdonjogát a haladó biztonsági funkciók használatához, amelyek a **Dell adatvédelem | Elérés** és a TPM segítségével vehetők igénybe.

Az **Eszközkezelés** Trusted Platform Module ablaka csak akkor jelenik meg, ha a rendszer TPM-et érzékel.

TPM-kezelés
Ezek a funkciók lehetővé teszik a rendszergazda számára a TPM kezelését.

Állapot
Megjeleníti a TPM *aktív* vagy *inaktív* állapotát. Az „Aktív” állapot azt jelenti, hogy megtörtént a TPM engedélyezése a BIOS-ban, és az készen áll a beállításra (azaz át lehet venni a tulajdonjogot). A TPM nem kezelhető és nem lehet hozzáférni biztonsági funkcióihoz, ha a TPM nem aktív (engedélyezett).

Ha a rendszer érzékeli a TPM-et, de az nem aktív (engedélyezett), akkor ezen ablak **aktiválás** hivatkozására kattintva a BIOS-ba való belépés nélkül engedélyezheti. A TPM ezen funkcióval történő engedélyezése után a számítógépet újra kell indítani. Újraindítás közben a rendszer bizonyos esetekben kéri a változtatások elfogadását.

MEGJEGYZÉS: Előfordulhat, hogy nem minden platform támogatja a TPM ezen alkalmazásból való engedélyezését (aktiválását). Ha ez nem támogatott, engedélyeznie kell a rendszer BIOS-ában. Ehhez indítsa újra a rendszert, és mielőtt a Windows betöltődne, nyomja meg az **F2** billentyűt a BIOS beállításokba való belépéshez, majd navigáljon a Biztonság>TPM biztonság pontra, és aktiválja a TPM-et.

Itt lehetősége van a TPM *deaktiválására* is: ehhez kattintson a **deaktiválás** hivatkozásra. A TPM deaktiválása megszünteti annak elérhetőségét a haladó biztonsági funkciók számára. A deaktiválás azonban egyetlen TPM beállítást sem módosít, ahogy semmilyen TPM-ben tárolt információ vagy kulcs törlését vagy módosítását sem hajtja végre.

Saját tulajdonú
Megjeleníti a tulajdonjog állapotát („saját tulajdonú”), és lehetővé teszi a TPM tulajdonos létrehozását vagy megváltoztatását. A TPM tulajdonjogot a TPM biztonsági funkcióinak elérhetősége érdekében kell létrehozni. Mielőtt létre lehetne hozni a tulajdonjogot, engedélyezni (aktiválni) kell a TPM-et.

A tulajdonjog létrehozási folyamatának keretében a (rendszergazdai jogosultságokkal rendelkező) felhasználó létrehozza a TPM tulajdonosi jelszót. A jelszó meghatározásával a tulajdonjog beállítása megtörtént, és a TPM használatra kész.

MEGJEGYZÉS: A TPM tulajdonosi jelszónak meg kell felelnie rendszere Windows-jelszavakra vonatkozó bonyolultsági szabályainak.

Fontos! Fontos, hogy ne veszítse el, vagy ne felejtse el a TPM tulajdonosi jelszót, mivel azt meg kell adni a TPM haladó biztonsági funkcióihoz való hozzáféréskor a **Dell adatvédelem | Elérés** alkalmazásban.

Zárolva
Megjeleníti a TPM *zárolva* vagy *feloldva* állapotát. A „Zárolás” a TPM biztonsági funkciója; a TPM a TPM tulajdonosi jelszó megadott számú helytelen beírása után lép zárolt állapotba. A TPM tulajdonosa itt oldhatja fel a TPM-et, melyhez meg kell adnia a TPM tulajdonosi jelszót.

MEGJEGYZÉSEK:

- Ha hibaüzenetet kap arról, hogy nem lehetett létrehozni a TPM tulajdonjogát, törölje a TPM-et a rendszer BIOS-ában, és próbálja meg ismét létrehozni a tulajdonjogot. A TPM törléséhez indítsa újra a számítógépet, az archiválás kezdetekor nyomja meg az **F2** billentyűt a BIOS beállítások eléréséhez, majd navigáljon a Biztonság>TPM biztonság helyre.
- Ha arról kap hibaüzenetet, hogy nem lehetett megváltoztatni a TPM tulajdonosi jelszót, archiválja a TPM adatokat (azonosítók archiválása), törölje a TPM-et a BIOS-ban, hozza létre újra a TPM tulajdonjogát, és állítsa vissza a TPM adatokat (azonosítók visszaállítása).
- Egy megadott hibaüzenettel kapcsolatban további információkért keresse fel a wave.com/support/Dell oldalt.

Dell ControlVault®

A Dell ControlVault® (CV) a felhasználók pre-Windows bejelentkezés során használatos azonosítóinak (pl. a felhasználói jelszavak vagy beolvasott ujjlenyomat-adatok) biztonságos tárolóhardvere. Az **Eszközkezelés** ControlVault ablaka csak akkor jelenik meg, ha a rendszer ControlVault jelenlétét érzékeli.

A ControlVault kezelése

Ezek a funkciók a rendszer ControlVault hardverének kezelését teszik lehetővé a rendszergazda számára.

Állapot
Megjeleníti a ControlVault *aktív* vagy *inaktív* állapotát. Az „Inaktív” állapot azt jelenti, hogy a ControlVault nem érhető el a rendszerben történő tárolás céljából. Nézzen utána a Dell rendszer dokumentációjában, hogy miként lehet megállapítani a rendszerben a ControlVault jelenlétét.

Jelszó
Azt jelzi, hogy be lett-e állítva a ControlVault rendszergazdai jelszó, és lehetővé teszi a jelszó létrehozását vagy megváltoztatását (ha az már beállításra került). Kizárólag rendszergazdák állíthatják be vagy módosíthatják ezt a jelszót. ControlVault rendszergazdai jelszót kell beállítani a következők végrehajtásához:

- Azonosítóarchiválás vagy -visszaállítás végrehajtása.
- Felhasználói adatok törlése (az összes felhasználó esetén).

MEGJEGYZÉS: Ha archiválási vagy visszaállítási kísérlet történik, amikor nincs beállítva a ControlVault rendszergazdai jelszó, a rendszer kéri annak létrehozását (ha a felhasználó rendszergazda).

Beolvasott felhasználók
Jelzi, hogy a felhasználók közül rendelkezik-e valaki beolvasott, ControlVault által aktuálisan tárolt bejelentkezési azonosítókkal (pl. jelszavak, ujjlenyomat- vagy smartcardadatok).

Felhasználói adatok törlése
Előfordulhat, hogy a ControlVault által tárolt adatokat valamikor törölni kell, például ha a felhasználóknak problémáik vannak a pre-Windows hitelesítői azonosítók használata vagy beolvasása során. Ebben az ablakban a ControlVault által tárolt összes adat törölhető egyetlen felhasználó vagy az összes felhasználó esetében.

A platform összes felhasználói adatának törléséhez be kell írni a ControlVault rendszergazdai jelszót. Ha pre-Windows azonosító is be lett olvasva, akkor a rendszerjelszót (pre-Windows jelszót) is be kell írnia. Ha törli az összes felhasználói adatot, a ControlVault rendszergazdai jelszó és rendszerjelszó alaphelyzetbe áll – ne feledje, hogy ez az egyetlen módja a ControlVault rendszergazdai jelszó törlésének.

MEGJEGYZÉS: Miután törölte az összes felhasználói adatot, a rendszer felszólítására újra kell indítania a számítógépet. Az újraindítás fontos a rendszer megfelelő működése érdekében.

A ControlVault rendszergazdai jelszót egyetlen felhasználó azonosítóinak törléséhez nem kell beállítani. Amikor a **felhasználói adatok törlése** gombra kattint, ki kell választania azt a felhasználót, akinek a ControlVault azonosítóit törölni kívánja. Miután kiválasztott egy felhasználót, be kell írnia a rendszerjelszót (de csak abban az esetben, ha be lettek olvasva pre-Windows azonosítók).

MEGJEGYZÉSEK:

- Ha hibaüzenetet kap arról, hogy nem lehet létrehozni a ControlVault rendszergazdai jelszót, archiválnia kell az azonosítókat, törölnie kell az összes felhasználói adatot a ControlVault hardverről, újra kell indítania a számítógépet, és meg kell kísérelnie a jelszó újbóli létrehozását.
- Ha arról kap hibaüzenetet, hogy az azonosítókat egy felhasználó esetében nem lehetett törölni a ControlVault hardverről, akkor archiválja az azonosítókat, próbálja meg törölni az összes felhasználói adatot, és próbálja meg ismét törölni az adatokat az adott felhasználó esetében.
- Ha hibaüzenetet kap arról, hogy az azonosítókat az összes felhasználó esetében nem lehetett törölni a ControlVault hardverről, akkor érdemes megfontolnia a rendszer visszaállítását. **Fontos!** Visszaállítás végrehajtása előtt olvassa el a rendszer-visszaállítás súgótémakört, mert ez a művelet az ÖSSZES felhasználó biztonsági adatát törli.
- Ha arról kap hibaüzenetet, hogy a ControlVault és a TPM adatok archiválása nem sikerült, tiltsa le a TPM-et a rendszer BIOS-ban. Ennek végrehajtásához indítsa újra a számítógépet, nyomja meg az **F2** billentyűt az archiválás kezdetekor a BIOS beállítások eléréséhez, majd navigáljon a Biztonság>TPM biztonság helyre. Ezután engedélyezze újra a TPM-et, és próbálja újra archiválni a ControlVault adatokat.
- Egy megadott hibaüzenettel kapcsolatban további információkért keresse fel a wave.com/support/Dell oldalt.

Self-Encrypting Drive egységek: Haladó

A **Dell adatvédelem | Elérés** kezeli a self-encrypting drive egységek hardver alapú biztonsági funkcióit, amelyek beépített titkosítással rendelkeznek a meghajtó hardverében. Ez a kezelési lehetőség biztosítja, hogy a titkosított adatokhoz kizárólag a jogosult felhasználók férhessenek hozzá, ha a meghajtó zárolása engedélyezve van.

Az **Eszközkezelés** Self-Encrypting drive ablaka csak akkor jelenik meg, amikor egy vagy több self-encrypting drive egység (SED) jelen van a rendszerben.

Fontos! Miután megtörtént a meghajtó beállítása, a self-encrypting drive adatvédelem és a meghajtó zárolása „engedélyezve vannak”.

A meghajtó kezelése

Ezek a funkciók lehetővé teszik a meghajtó-rendszergazda számára a meghajtó biztonsági beállításainak kezelését. A meghajtó biztonsági beállításainak módosításai a meghajtó kikapcsolása után lépnek érvénybe.

Adatvédelem

Megjeleníti a self-encrypting drive egység adatvédelmének *engedélyezett* vagy *letiltott* állapotát. Az „engedélyezett” állapot azt jelenti, hogy a meghajtóbiztonság be van állítva; amíg azonban a meghajtó *zárolása* be van kapcsolva, a felhasználóknak nem kell azonosítaniuk magukat a meghajtón a pre-Windows elérés során.

Itt lehetősége van a self-encrypting drive adatvédelem letiltására. Amikor le van tiltva, a self-encrypting drive összes haladó biztonsági beállítása ki van kapcsolva, és a meghajtó közönséges meghajtóként működik. Az adatvédelem letiltása az összes biztonsági beállítást is törli, a meghajtó rendszergazdájának és felhasználóinak azonosítóit is beleértve. Ez a funkció azonban nem módosítja vagy törli a meghajtón található felhasználói adatokat.

Zárolás

Megjeleníti a self-encrypting drive egység(ek) *engedélyezett* vagy *letiltott* állapotát. A zárolt meghajtó viselkedésével kapcsolatban a Self-Encrypting Drive témakörben találhatók bővebb információk.

Előfordulhat, hogy szükségessé válik a meghajtó zárolásának átmeneti letiltása, amely elvégezhető innen. Ez azonban nem javasolt, mivel ekkor nem kötelező az azonosítás a meghajtó elérésekor, ha a meghajtó zárolása letiltott állapotban van, így a platform bármely felhasználója elérheti a meghajtó adatait. A meghajtó zárolásának letiltása nemtöröl semmilyen biztonsági beállítást, a meghajtó rendszergazdájának és a felhasználóknak az azonosítóit, illetve bármilyen meghajtón lévő felhasználói adatot is beleértve.

VIGYÁZAT! Ha eltávolítja a **Dell adatvédelem | Elérés** alkalmazást, először le kell tiltania a self-encrypting drive adatvédelmet, és meg kell szüntetnie a meghajtó zárolását.

Meghajtó-rendszergazda

Megjeleníti a meghajtó aktuális rendszergazdáját. A meghajtó rendszergazdája itt változtathatja meg, hogy melyik felhasználó a meghajtó rendszergazdája. Az új rendszergazdának olyan érvényes Windows-felhasználónak kell lennie a rendszerben, aki rendszergazdai jogosultságokkal rendelkezik. A rendszerben csak egy meghajtó-rendszergazda lehet.

Meghajtófelhasználók

Megjeleníti a beolvasott meghajtófelhasználókat, valamint a jelenleg beolvasott felhasználók számát. A felhasználók maximális támogatott száma a self-encrypting drive egységen alapul (aktuálisan 4 felhasználó a Seagate meghajtók és 24 a Samsung meghajtók esetén).

Windows jelszó-szinkronizálás

A Windows jelszó-szinkronizálás (WPS) funkció automatikusan a Windows-jelszavukkal megegyező értékre állítja be a felhasználók Self-Encrypting Drive jelszavát. Ez a funkció nem lép életbe a meghajtó rendszergazdájánál, csak a meghajtó felhasználóira vonatkozik. A WPS funkció olyan vállalati környezetben használható, ahol a jelszavakat rendszeres időközönként (pl. 90 naponta) meg kell változtatni; ennek a beállításnak az engedélyezésével az összes felhasználó self-encrypting drive jelszava automatikusan frissül, amikor Windows-jelszavuk megváltozik.

MEGJEGYZÉS: Amikor engedélyezve van a Windows jelszó-szinkronizálás (WPS), akkor nem lehet megváltoztatni a felhasználók Self-Encrypting Drive jelszavát; a felhasználók Windows-jelszavát módosítani kell a meghajtójelszó automatikus frissítéséhez.

Emlékezzen az utolsó felhasználónévre

Amikor engedélyezve van ez a beállítás, alapértelmezés szerint az utoljára beírt felhasználónév jelenik meg a pre-Windows hitelesítési képernyő **Felhasználónév** mezőjében.

Felhasználónév kiválasztása

Amikor engedélyezve van ez a beállítás, a felhasználók megtekinthetik a meghajtó összes felhasználónevét a pre-Windows hitelesítési képernyő **Felhasználónév** mezőjében.

Kriptografikus törlés

Ezt a beállítást lehet alkalmazni a self-encrypting drive egység összes adatának „törléséhez”. Ez a beállítás nem törli ténylegesen az adatokat, de az adatok titkosítására használt kulcsokat eltávolítja, ezáltal pedig használhatatlanná teszi ezeket az adatokat. A kriptografikus törlés után nem lehet helyreállítani a meghajtó törölt adatait, a self-encrypting drive adatvédelem is le van tiltva, és a meghajtó készen áll a más célra való átállításra.

MEGJEGYZÉSEK:

- Ha bármilyen hibaüzenetet kap a self-encrypting drive kezelési funkcióival kapcsolatban, kapcsolja ki teljesen a számítógépet (az újraindítás nem elegendő), majd kapcsolja be újra a gépet.
- Egy megadott hibaüzenettel kapcsolatban további információkért keresse fel a wave.com/support/Dell oldalt.

Azonosítóeszköz-információk

Az Azonosítóeszköz-információk ablaka az **Eszközkezelés** képernyőjén belül az összes csatlakoztatott azonosítóeszközzel (pl. ujjlenyomat-leolvasóval, hagyományos vagy contactless smartcard olvasóval) kapcsolatos információkat és azok rendszeren belüli állapotát jeleníti meg.

Műszaki támogatás

A **Dell adatvédelem | Elérés** szoftver műszaki támogatása a következő oldalon érhető el: http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP

A **Dell adatvédelem | Elérés** alkalmazás a Wave Systems Trusted Computing Group (TCG)-enabled Kriptográfiai szolgáltatót (CSP) tartalmazza, mely mindig elérhető, amikor szükség van Kriptográfiai szolgáltatóra (CSP) – akár közvetlenül az alkalmazásból meghívva, akár a telepített CSP-k közül kiválasztva. Amikor lehetséges, mindig a „Wave TCG-Enabled CSP" szolgáltatót válassza annak érdekében, hogy a TPM állítsa elő a kulcsokat, a kulcsok és jelszavak kezelését pedig a **Dell adatvédelem | Elérés** alkalmazás végezze.

A Wave Systems TCG-enabled CSP lehetővé teszi, hogy az alkalmazások az MSCAPI felületen keresztül közvetlenül használják a TCG-kompatibilis platformok szolgáltatásait. A TCG-enhanced MSCAPI CSP modul teszi lehetővé az aszimmetrikus kulcs használatát a TPM-nél, és kihasználja a TPM kínálta fejlett biztonsági szolgáltatásokat, függetlenül attól, hogy milyen forgalmazóspecifikus igényeket kell kielégíteni a Trusted Software Stack (TSS) miatt.

MEGJEGYZÉS: Ha a Wave TCG-enabled CSP által létrehozott TPM kulcsok jelszót igényelnek, és a felhasználó létrehozott egy TPM mesterjelszót, az egyedi kulcsjelszavak véletlenszerűen kerülnek létrehozásra és tárolásra a TPM jelszótárolóban.