Dell Data Protection | Access Home

Pagina de start **Dell Data Protection | Access** heste punctul de plecare pentru accesarea funcţiilor acestei aplicaţii. Din această fereastră, puteţi accesa următoarele:

System Access Wizard
Opţiuni de acces
Unitate cu autocriptare
Opţiuni de configurare avansate

În colţul din dreapta jos a ferestrei este un link numit **configurări avansate** pe care dacă faceţi clic accesaţi opţiunile de configurare avansate.

Din opţiuni de configurare avansate, puteţi face clic pe link-ul **acasă**din colţul din dreapta jos a ferestrei pentru a reveni la pagina de start.

System Access Wizard

System Access Wizard se lansează automat când aplicaţia **Dell Data Protection | Access** este lansată pentru prima dată. Această aplicaţie wizard vă va ghida în configurarea tuturor aspectelor de securitate pe sistem, inclusiv modul (de ex., doar parolă sau parolă şi amprentă) şi momentul în care(în Windows, pre-Windows sau ambele) doriţi să vă autentificaţi în sistem. În plus, dacă sistemul are o unitate cu autocriptare, puteţi să să-l configuraţi cu ajutorul acestei aplicaţii wizard.

Funcţii de administrare

Utilizatorii cărora le-au fost conferite drepturi de administrator Windows pe sistem au drepturi de a realiza următoarele funcţii în **Dell Data Access | Protection**, pe care utilizatorii standard nu le pot face:

- Setare / schimbare parolă de sistem (pre-Windows)
- Setare / schimbare parolă hard disk
- Setare / schimbare parolă administrator
- Setare / schimbare parolă proprietar TPM
- Setare / schimbare parolă administrator ControlVault
- Resetare sistem
- Arhivare şi restabilire referinţe
- Setare / schimbare PIN smartcard de administrator
- Ştergere / resetare smartcard
- Activare / dezactivare autentificare securizată Dell în Windows
- Setare politică de autentificare Windows
- Gestionare unitate cu autocriptare, inclusiv:
    - Activare / dezactivare blocare unitate cu autocriptare
    - Activare / dezactivare sincronizare parole Windows (WPS)
    - Activare / dezactivare autentificare unică (SSO)
    - Efectuare ştergere criptografică

Gestionare de la distanţă

Organizaţia dumneavoastră poate configura un mediu în care funcţiile de securitate ale aplicaţiei **Dell Data Protection | Access** pe platforme multiple sunt gestionate central (adică gestionare de la distanţă). În acest caz, infrastructura de securitate Windows, cum ar fi Director activ, pot fi folosite pentru a gestiona în siguranţă funcţiile specifice ale **Dell Data Protection | Access**.

Când un computer este gestionat de la distanţă (de ex., "în proprietatea" administratorului de la distanţă), administraţia locală a funcţiei **Dell Data Protection | Access** va fi dezactivată; fereastra de gestionare a aplicaţiei nu va putea fi accesată la nivel local. Gestionarea următoarelor funcţii poate fi făcută de la distanţă:

- Trusted Platform Module (TPM)
- ControlVault
- Autentificare pre-Windows
- Resetare sistem
- BIOS Parole
- Politica de autentificare Windows
- Unităţi cu autocriptare
- Înregistrare amprentă şi smartcard

Pentru a cere mai multe informaţii referitoare la folosirea Wave Systems' EMBASSY® Remote Administration Server (ERAS) pentru gestionare de la distanţă, contactaţi agentul local de vânzări Dell sau accesaţi dell.com.

Opţiuni de acces

Din fereastra Opţiuni de acces puteţi să configuraţii modalitatea prin care obţineţi acces la sistemul dumneavoastră.

Dacă aveţi configurată oricare din opţiunile **Dell Data Protection | Access**, acestea vor fi afişate pe pagina de start cu opţiunile disponibile (de ex., modificare parolă pentru autentificare în pre-Windows). Opţiunile disponibile sunt comenzi rapide, care, dacă se face clic pe ele, vă duc în fereastra adecvată pentru efectuarea unei sarcini specifice (de ex., modificarea parolei pentru autentificare în pre-Windows sau înregistrarea unei alte amprente).

Generalităţi
În primul rând, puteţi specifica când vă autentificaţi (în Windows, pre-Windows sau în ambele) şi modalitatea prin care vă autentificaţi. Puteţi alege una sau două opţiuni pentru modalitatea de autentificare; acestea includ combinaţii de amprentă, smartcard şi parolă. Opţiunile enumerate se bazează pe politicile de autentificare aplicate în mediul dumneavoastră şi ceea ce este compatibil cu platforma.

Amprentă
Dacă sistemul dumneavoastră conţine un cititor de amprente, puteţi să înregistraţi sau să actualizaţi amprente pentru a fi folosite la autentificarea în sistemul dumneavoastră. După ce aţi înregistrat amprentele, puteţi să treceţi degetul (degetele) înregistrat (înregistrate) prin faţa cititorului de amprente al sistemului dumneavoastră pentru a accesa pe sistem Windows, pre-Windows sau ambele (în funcţie de ce aţi specificat în Opţiunile generale de accesare). Consultaţi Înregistrare amprente utilizator pentru mai multe informaţii.

Autentificare în pre-Windows
Dacă aţi specificat că utilizatorii trebuie să se autentifice în pre-Windows, trebuie să configuraţi o Parolă de sistem (uneori denumită parola pentru pre-Windows) pentru a accesa pre-Windows. După ce aţi configurat acest lucru, administratorul poate modifica parola oricând.

De asemenea, puteţi dezactiva autentificarea în pre-Windows din acest ecran; pentru aceasta, trebuie să introduceţi parola de sistem actuală, să verificaţi dacă parola este corectă, şi apoi să faceţi clic pe butonul **Dezactivare**.

Smartcard
Dacă aţi specificat că utilizatorii trebuie să folosească un smartcard pentru autentificare, trebuie să înscrieţi una sau mai multe smartcard-uri tradiţionale (cu contact) sau contactless. Faceţi clic pe link-ul **Înscriere alt smartcard** pentru a lansa aplicaţia wizard pentru înscrierea de smartcard. Înscrierea înseamnă configurarea smartcard-ului dumneavoastră pentru autentificare.

După ce aţi înscris un smartcard, puteţi modifica sau configura un PIN pentru utilizarea acelui card folosind link-ul **Modificare sau configurare PIN pentru smartcard-ul meu**.

Autentificare pre-Windows

Când se configurează autentificarea pre-Windows, trebuie să vă autentificaţi (prin parolă, amprentă sau smartcard) când sistemul este pornit, înainte ca Windows să se încarce. Funcţia de autentificare în pre-Windows oferă securitate suplimentară sistemului, nelăsând utilizatorii neautorizaţi să compromită Windows şi să acceseze computerul (de ex, dacă a fost furat).

Din fereastra Autentificare pre-Windows, administratorii pot să configureze autentificarea pre-Windows, sau să creeze ori să modifice oparolă pre-Windows (sistem); dacă această parolă a fost deja configurată, puteţi dezactiva autentificarea pre-Windows din această fereastră. Configurarea autentificării pre-Windows va lansa o aplicaţie wizard care va efectua următoarele:

- Parolă de sistem: Se configurează o parolă de sistem (numită şi parolă pre-Windows) pentru acces în pre-Windows. Această parolă este folosită de asemenea ca şi copie de rezervă în cazuri în care un utilizator are factori de autentificare suplimentari (de exemplu, pentru a obţine acces la sistem dacă există o problemă cu senzorul de amprente).
- Amprentă sau Smartcard: Se configurează o amprentă sau un smartcard pentru autentificare în pre-Windows, şi se specifică dacă acest factor de autentificare va fi folosit în loc de sau suplimentar faţă de parola pre-Windows.
- Autentificare unică: În mod Implicit, autentificarea pre-Windows (parolă, amprentă sau smartcard) va fi folosită şi pentru autentificare automată în Windows (ceea ce este numită "Autentificare unică"). Pentru a dezactiva această funcţie, selectaţi caseta "Doresc să mă autentific încă o dată în Windows".
- Dacă o parolă BIOS pentru hard disk a fost configurată suplimentar faţă de o parolă pre-Windows, veţi avea şi opţiunea de a modifica sau de a dezactiva parola pentru hard disk.

NOTĂ: Nu toate cititoarele de amprente sunt disponibile pentru folosirea cu autentificarea pre-Windows. Dacă cititorul dumneavoastră nu este compatibil, veţi putea înregistra amprente doar pentru autentificare în Windows. Pentru a afla dacă un anumit cititor de amprente este compatibil, contactaţi administratorul sistemului sau accesaţi support.dell.com pentru o listă cu cititoare de amprente compatibile.

Dezactivare Autentificare pre-Windows
Puteţi dezactiva autentificarea pre-Windows şi din această fereastră; pentru aceasta, va trebui să introduceţi parola actuală pre-Windows (de sistem), să verificaţi dacă parola este corectă, apoi să faceţi clic pe butonul **Dezactivare**. Reţineţi că în momentul în care dezactivaţi autentificarea pre-Windows, orice amprente sau smartcard-uri înregistrate rămân înregistrate.

Înregistrare amprente

Utilizatorii pot înregistra sau actualiza amprente care pot fi utilizate pentru autentificarea în sistem, atât în pre-Windows cât şi în Windows. În tab-ul Amprente, imagini ale mâinii afişează degetele care au fost înregistrate, dacă există. Făcând clic pe link-ul **Înregistrare nouă**se lansează programul wizard de înregistrare a amprentelor, care vă ghidează în procesul de înregistrare. "Înregistrare" înseamnă salvarea amprentei pentru a fi folosită pentru autentificare. Trebuie să aveţi un cititor de amprente valabil corect instalat şi configurat pentru a înregistra amprente.

NOTĂ: Nu toate cititoarele de amprente pot fi folosite pentru autentificarea în pre-Windows. Un mesaj de eroare va fi afişat dacă încercaţi să vă înregistraţi în pre-Windows cu un cititor incompatibil. Pentru a afla dacă dispozitivul este compatibil, contactaţi administratorul de sistem sau accesaţi support.dell.com pentru o listă de cititoare de amprente compatibile.

Când înregistraţi amprente, vi se va cere să introduceţi parola Windows pentru a vă confirma identitatea. Dacă politica dumneavoastră o cere, va trebui să introduceţi şi parola pre-Windows (sistem) . Parola pre-Windows poate fi folosită pentru a obţine acces la sistem dacă există vreo problemă cu cititorul de amprente.

NOTE:

- Este recomandat să vă înregistraţi cel puţin două amprente pe parcursul procesului de înregistrare.
- Trebuie să vă asiguraţi că amprentele sunt înregistrate corect înainte de a activa funcţiile de autentificare pe bază de amprente.
- Dacă schimbaţi cititoarele de amprente pe un sistem, trebuie să reînregistraţi amprentele cu noul cititor. Nu se recomandă comutarea continuă între două dispozitive de amprente diferite.
- Dacă primiţi în mod repetat mesaje de genul "senzorul şi-a pierdut focalizarea" când înregistraţi amprente, e posibil ca cititorul de amprente să nu fie recunoscut de computer. În cazul în care cititorul de amprente este extern, deconectarea şi reconectarea sa deseori rezolvă această problemă.

Ştergere amprente înregistrate
Puteţi şterge amprentele înregistrate făcând clic pe link-ul **Ştergere amprentă** sau făcând clic pe (pentru a deselecta) un deget înregistrat în aplicaţia wizard de înregistrare a amprentelor.

Pentru a şterge un anumit utilizator care are amprenta înregistrată pentru autentificare în pre-Windows, administratorul poate deselecta toate amprentele înregistrate ale acelui utilizator.

NOTĂ: Dacă primiţi orice erori pe parcursul procesului de înregistrare a amprentelor, puteţi să consultaţi wave.com/support/Dell pentru detalii suplimentare.

Înscriere Smart Carduri

Dell Data Protection | Access vă oferă opţiunea de utilizare a unui smartcard tradiţional (cu contact) sau contactless pentru a vă autentifica în contul Windows sau pentru autentificare în pre-Windows. În tab-ul Smartcard, faceţi clic pe link-ul **Înscriere alt smartcard** pentru a lansa programul wizard Smartcard Enrollment, care vă ghidează în procesul de înscriere. "Înscriere" înseamnă configurarea smartcard-ului dumneavoastră pentru a fi folosit în autentificare.

Trebuie să aveţi un dispozitiv de autentificare pe bază de smartcard corect instalat şi configurat pentru a efectua înscrierea.

NOTĂ: Pentru a afla dacă un anumit dispozitiv este compatibil, contactaţi administratorul de sistem administrator sau accesaţi support.dell.com pentru o listă de smartcard-uri compatibile.

Înscriere
Când înscrieţi un smartcard vi se va cere să introduceţi parola Windows pentru a vă fi verificată identitatea. Dacă politica dumneavoastră o cere, va trebui să introduceţi şi parola pre-Windows (sistem) . Parola Pre-Windows poate fi folosită pentru a obţine acces la sistem dacă este vreo problemă cu cititorul de smartcard.

În timpul înscrierii, vi se va cere PIN-ul smartcard-ului, dacă o astfel de parolă a fost setată. Dacă politica dumneavoastră cere un PIN şi nu a fost setat încă unul, vi se va cere să creaţi unul.

NOTĂ:

- După ce un utilizator este înscris pentru a utiliza smartcard în pre-Windows, el/ea nu mai poate fi şters/ştearsă.
- Utilizatorii standard pot modifica codul PIN al utilizatorului unui smartcard, iar administratorul poate modifica atât codul PIN al administratorului cât şi codul PIN al utilizatorilor.
- De asemenea, administratorul poate reseta un smartcard; după ce este resetat, smartcard-ul nu poate fi folosit pentru autentificare în Windows sau în pre-Windows până ce nu este reînscris.

NOTĂ: Pentru autentificarea pe bază de certificat TPM, administratorii pot înscrie certificate TPM prin procesul Microsoft Windows de înscriere a smartcard-ului. Administratorii trebuie să selecteze "Wave TCG-Enabled CSP" ca furnizorul de servicii criptografice (CSP) în loc de smartcard CSP în vederea asigurării compatibilităţii cu această aplicaţie. De asemenea, autentificarea securizată trebuie activată cu Politica tipului de autentificare corectă pentru client.

NOTĂ: Dacă primiţi o eroare că Serviciul Smartcard Service nu rulează, puteţi să începeţi / reîncepeţi acest serviciu, făcând următoarele acţiuni:

- Navigaţi la fereastra Administrative Tools (Instrumente administrative) din Control Panel (Panou de comandă), selectaţi Service (Serviciu), apoi faceţi clic-dreapta pe smartcard şi selectaţi Start sau Restart.
- Pentru informaţii mai detaliate despre un anumit mesaj de eroare, accesaţi wave.com/support/Dell.

Unitate cu autocriptare

Dell Data Protection | Access gestionează funcţiile de securitate bazate pe hardware alaunităţilor cu autocriptare, care au au încorporat în unitatea hardware funcţia de criptare a datelor. Această funcţie este folosită pentru a asigura că doar utilizatorii autorizaţi pot accesa datele criptate (când este activată blocarea unităţii).

Fereastra Unitate cu autocriptare este accesată făcând clic pe tab-ul de jos **Unitate cu autocriptare**. Acest tab este afişat doar când una sau mai multe unităţi cu autocriptare (SED) sunt prezente în sistem.

Faceţi clic pe link-ul**Configurare**pentru aplicaţia wizard de configurare a unităţii cu autocriptare. În această aplicaţie wizard, veţi crea o parolă de administrator al unităţii, veţi crea o copie de rezervă a acestei parole, şi veţi aplica setările dumneavoastră de criptare a unităţii. Doar administratorii de sistem pot accesa aplicaţia wizard de configurare a unităţii cu autocriptare.

Important! După ce unitatea cu autocriptare a fost configurată, sunt "activate" protecţia datelor şiblocarea unităţii. Când o unitate este blocată, se aplică următorul comportament:

- Unitatea intră în modul*blocat* când alimentarea este oprită.
- Unitatea nu va reporni decât dacă utilizatorul introduce numele de utilizator şi parola (sau amprenta) corectă la ecranul de autentificare în pre-Windows. Înainte de activarea blocării unităţii, datele de pe unitate sunt accesibile oricărui utilizator de pe computer.
- Unitatea este securizată chiar dacă este conectată la un alt computer ca o unitate secundară; este necesară autentificarea pentru a accesa datele de pe unitate.

Odată ce unitatea a fost configurată, fereastra Unitate cu autocriptare va afişa unitatea (unităţile) şi un link pentru utilizatori pentru ca aceştia să-şi modifice parola. Dacă sunteţi un administrator al unităţii, veţi putea, de asemenea, să adăugaţi sau să ştergeţi utilizatorii unităţii din această fereastră. Dacă există o unitate externă care a fost configurată, se va afişa pe fereastră că se poate debloca.

NOTĂ: Pentru a bloca o unitate secundară, unitate externă, unitatea trebuie să fie oprită independent de computer.

Administratorul unităţii poate administra setările unităţii în **Configurare avansată>Dispozitive**. Pentru mai multe informaţii, accesaţi Gestionarea dispozitivului - Unităţi cu autocriptare.

Configurare unitate

Aplicaţia wizard de configurare a unităţii cu autocriptare vă va ghida în procesul de configurare a unităţii (unităţilor). Următoarele concepte sunt important de avut în vedere la efectuarea acestui proces.

Administratorul unităţii
Primul utilizator cu drepturi de administrator de sistem care configurează accesul la unitate (şi configurează parola de administrator al unităţi) devine administratorul unităţii, acesta este singurul utilizator cu dreptul de a face modificări la accesul la unitate. Pentru a vă asigura că primul utilizator este configurat în mod intenţionat ca administrator al unităţii, trebuie să selectaţi căsuţa "Înţeleg" pentru a continua cu acest pas.

Parola de administrator alunităţii
Această aplicaţie wizard vă va cere să creaţi o parolă de administrator al unităţii şi să reintroduceţi parola pentru confirmare. Trebuie să introduceţi parola Windows pentru verificarea identităţii dumneavoastră, înainte să puteţi crea parola de administrator al unităţii. Utilizatorul curent Windows trebuie să aibă drepturi de administrator pentru a crea această parolă.

Referinţe de rezervă ale unităţii
Introduceţi o locaţie, sau faceţi clic pe butonul **Browse** pentru a selecta o locaţie, pentru a salva o copie de rezervă a referinţelor de administrator al unităţii.

IMPORTANT**!**

- Vă recomandăm insistent să faceţi copii de rezervă a acestor referinţe şi să faceţi aceste copii pe o unitate diferită de hard disk-ul primar (de ex., suporturi amovibile). În caz contrar, dacă pierdeţi accesul la unitate, nu veţi mai putea să accesaţi copia de rezervă.
- Odată ce aţi terminat configurarea unităţii, oriceutilizator va trebui să introducă numele de utilizator şi parola (sau amprenta) corectă, înainte ca Windows să se încarce, pentru a accesa sistemul la următoarea sa pornire.

Adăugare utilizator al unităţii
Administratorul unităţii poate adăuga alţi utilizatori pe unitate care sunt utilizatori Windows valizi. La adăugarea utilizatorilor pe unitate, administratorul are opţiunea de a cere utilizatorului să reseteze parola la prima sa autentificare. Utilizatorului i se va cere să reseteze parola pe ecranul de autentificare pre-Windows înainte de blocarea unităţii.

Setări avansate

- *Autentificare unică* - În mod implicit, parola pentru unitatea cu autocriptare pe care aţi introdus-o în pre-Windows pentru autentificarea în unitate, va fi utilizată şi pentru a vă autentifica automat în Windows (numită "Autentificare unică"). Pentru a dezactiva această funcţie, selectaţi căsuţa "Vreau să mă autentific încă o dată la pornirea Windows" când configuraţi setările unităţii.
- *Autentificare pe bază de amprente* - Pe platforme compatibile, puteţi specifica că doriţi să vă autentificaţi în unitatea cu autocriptare folosind o amprentă în locul unei parole.
- *Sleep/Standby (S3) Asistenţă* (dacă este compatibilă cu platforma) - Dacă este activată, unitatea cu autocriptare poate fi plasată în siguranţă în modul Sleep/Standby(numit şi mod S3) şi va cere autentificare în pre-Windows când revine din modul Sleep/Standby.

NOTE:

- Când asistenţa S3 este activată, parolele unităţii cu autocriptare este supusă eventualelor limitări de parolă BIOS. Vă rugăm să consultaţi fabricantul hardware-ului din sistem pentru mai multe informaţii privind limitările specifice ale parolei BIOS care pot exista în sistem.
- Nu toate unităţile cu autocriptare sunt compatibile cu modul S3. În timpul configurării unităţii, veţi fi anunţat dacă unitatea este sau nu compatibilă cu modul Standby/Sleep. Pentru unităţi care nu sunt compatibile cu acest mod, cererile Windows S3 vor fi transformate automat în cereri de hibernare, dacă modul de hibernare este activat (vă recomandăm insistent să activaţi modul de hibernare pe computer).
- La prima autentificare după ce opţiunea Autentificare unică (SSO) a fost setată, procesul se va opri la solicitarea de autentificare în Windows. Vi se va cere să introduceţi forma de autentificare Windows, care va fi stocată în condiţii de securitate pentru încercările de autentificare în Windows ulterioare. La pornirea viitoare a sistemului, SSO vă va autentifica automat în Windows. Acelaşi proces este necesar şi când modalitatea de autentificare a unui utilizator Windows (parolă, amprentă, PIN smartcard) se modifică. În cazul în care computerul este pe un domeniu, şi acel domeniu are o politică care cere apăsarea ctrl+alt+del pentru autentificare în Windows, această politică va fi respectată.

ATENŢIE: Dacă dezinstalaţi aplicaţia **Dell Data Protection | Access**, întâi trebuie să dezactivaţi protecţia datelor de pe unitatea cu autocriptare şi să deblocaţi unitatea.

Funcţii utilizator SED

Administratorii unităţii cu autocriptare realizează întreaga gestiune a securităţii şi a utilizatorilor unităţii. Utilizatorii unităţii care nu sunt administratorul unităţii pot realiza doar următoarele activităţi:

- Schimbarea propriei parole pentru unitate
- Deblocarea unei unităţi

Aceste activităţi pot fi accesate din tab-ul**Unitate cu autocriptare** în **Dell Data Protection | Access**.

Schimbare parolă
Această funcţie permite utilizatorilor înregistraţi să-şi creeze o nouă parolă de autentificare pe unitate. Trebuie să introduceţi actuala parolă pentruunitatea cu autocriptare înainte ca parola pentru unitate să fie setată la noua valoare.

NOTE:
- Aplicaţia va stabili lungimea parolei Windows şi politicile de complexitate ale parolelor, dacă acestea sunt activate. Dacă politicile de parole Windows nu sunt activate, lungimea maximă a unei parole pentru o unitate cu autocriptare este de 32 de caractere. Reţineţi că această lungimea maximă este de 127 de caractere dacă S3 (Sleep/Standby) nu este activată.
- Parola pentru unitatea cu autocriptare a unui utilizator este diferită de parola Windows a acestuia. Când se modifică sau se resetează parola Windows a unui utilizator, acest lucru nu afectează parola pentru unitate a utilizatorului, decât dacă a fost activată Sincronizarea parolelor Windows. Consultaţi Dispozitive: Unităţi cu autocriptare pentru detalii.
- Pe unele tastaturi non-engleze, există un set de caractere restricţionate care nu pot fi folosite pentru parola pentru unitatea cu autocriptare. Dacă parola Windows conţine vreunul dintre caracterele restricţionate, şi este activată sincronizarea parolelor Windows, sincronizarea va eşua şi va fi afişat un mesaj de eroare.

Deblocare unitate:
Deblocarea unităţii permite unui utilizator înregistrat al unităţii să deblochezeo unitate blocată. Dacă blocarea unităţii este activată, unitatea se blochează de fiecare dată când PC-ul este oprit. Când sistemul este repornit, trebuie să vă autentificaţi în unitate introducând parola în ecranul de autentificare pre-Windows.

NOTE:
- Este posibil să nu se poată intra într-un mod de lucru economic (adică Sleep/Standby sau Hibernare) dacă pe computer sunt active concomitent mai multe conturi de utilizator ai unităţii cu autocriptare.
- Pe ecranul de autentificare pre-Windows, cuvintele "Utilizatorul 1","Utilizatorul 2", etc. înlocuiesc numele utilizatorilor de unitate în versiunile aplicaţiei care sunt localizate pentru următoarele limbi: chineză, japoneză, coreeană şi rusă.

Opţiuni configurare avansată

Opţiunile avansate din **Dell Data Protection | Access** permite unui utilizator cu drepturi de administrator să gestioneze următoarele aspecte ale aplicaţiei:

Maintenance
Parole
Dispozitive

NOTĂ: Doar utilizatorii cu drepturi de administrator pot efectua modificări în Opţiunile de configurare avansate; utilizatorii standard pot vizualiza aceste setări, dar nu pot face nicio modificare.

Maintenance

Fereastra Maintenance poate fi folosită de administratori pentru a configura preferinţele de autentificare în Windows, pentru a reseta un sistem în vederea folosirii sale în alt scop, sau pentru a arhiva sau restabili referinţele utilizatorului stocate în hardware-ul de securitate a sistemului. Pentru detalii, consultaţi următoarele teme:

Preferinţe acces
Resetare sistem
Arhivă referinţe & Restabilire

Access Preferences

Fereastra Access Preferences permite administratorului să specifice preferinţele de autentificare în Windows pentru toţi utilizatorii sistemului.

Activitate Autentificare securizată Dell
Opţiunea de a înlocui ecranul standard Windows ctrl-alt-delete vă permite să folosiţi factori de autentificare diferiţi în loc (sau în plus faţă de) parola Windows pentru a accesa Windows. Puteţi alege să adăugaţi o amprentă ca un al doilea factor de autentificare pentru a întări siguranţa procesului de autentificare Windows. De asemenea, pentru autentificarea în Windows se pot adăuga factori de autentificare suplimentari, inclusiv un smartcard sau un certificat TPM.

NOTE:

- Activarea autentificării securizate afectează toţi utilizatorii sistemului.
- Se recomandă activarea acestei opţiuni DUPĂ ce utilizatorii şi-au înregistrat amprentele şi si-au înscris smartcard-ul.
- La prima autentificare după setarea acestei opţiuni, vi se va cere să vă autentificaţi în Windows conform politicii standard, iar la următoarea pornire va trebui să folosiţi noul (noii) factor(i) de autentificare.

Dezactivare autentificare securizată Dell
Această opţiune dezactivează toate funcţiile **Dell Data Protection | Access** pentru autentificare în Windows. Când aceasta este selectată, veţi reveni la politica standard de autentificare în Windows.

NOTE:

- Dacă primiţi o eroare referitoare la autentificarea securizată în Windows când încercaţi să vă autentificaţi, dezactivaţi şi reactivaţi opţiunea de autentificare securizată Dell.
- Pentru informaţii mai detaliate despre un anumit mesaj de eroare, accesaţi wave.com/support/Dell.

Resetare sistem

Funcţia de Resetare sistem este folosită pentru a şterge toate toate datele utilizatorilor de pe toate hardware-urile de securitate ale platformei; aceasta se foloseşte, de exemplu, pentru utilizarea unui computer în alt scop. Această opţiune va şterge toate parolele de pe sistem, cu excepţia parolelor de utilizator Windows, precum şi toate datele din dispozitivele de hardware (adică ControlVault, TPM şi cititoare de amprente). Pentru unităţi cu autocriptare această funcţie dezactivează şi protecţia datelor pentru ca datele de pe unitate să fie accesibile.

Trebuie să confirmaţi că înţelegeţi că urmaţi să resetaţi sistemul, apoi faceţi clic pe **Mai departe**. Pentru a reseta sistemul, vi se va cere să introduceţi parola pentru fiecare dispozitiv de securitate, dacă au fost configurate.

- TPM Proprietar
- Administrator ControlVault
- Administrator BIOS
- BIOS Sistem (pre-Windows)
- Hard disk (BIOS)
- Administrator unitate cu autocriptare

NOTĂ: Pentru unităţile cu autocriptare, este necesară doar parola de administrator al unităţii, şi nu parolele tuturor utilizatorilor unităţii.

Important! Singura cale de a recupera oricare din datele şterse când aţi resetat sistemul este de restabilire dintr-o arhivă salvată anterior. Dacă nu aveţi o arhivă, aceste date nu pot fi recuperate. În cazul unei unităţi cu autocriptare, doar datele de configurare sunt şterse; nicio dată personală de pe unitate nu este ştearsă.

Arhivare referinţe & Restabilire

Funcţia Arhivare şi restabilire referinţe este utilizată pentru realizarea unei copii de rezervă şi restabilirea tuturor referinţelor (informaţii legate de autentificare şi criptare) stocate în ControlVault şi Trusted Platform Module (TPM). O copie de rezervă a acestor date este importantă pentru resetarea unui computer şi pentru a restabili date în cazul unei defecţiuni hardware. În acest caz, puteţi restabili uşor toate referinţele dumneavoastră pe noul computer dintr-un fişier de arhivă salvat.

Puteţi alege să arhivaţi sau să restabiliţi referinţe pentru un singur utilizator sau pentru toţi utilizatorii sistemului.

Referinţele utilizatorului constă din date utilizate în pre-Windows, cum ar fi amprente înregistrate şi smartcard-uri înscrise, şi cheie stocate în TPM. TPM va crea chei conform solicitărilor primite din partea aplicaţiilor securizate; de exemplu, generarea unui certificat digital va crea chei în TPM.

NOTĂ: Pentru a determina dacă e posibilă arhivarea cheilor TPM cu ajutorulDell Data Protection | Access, consultaţi documentaţia pentru aplicaţia securizată. În general, aplicaţiile care folosesc “Wave TCG-Enabled CSP” pentru a genera chei sunt compatibile.

Arhivare referinţe
Pentru a arhiva referinţe, trebuie să faceţi următoarele:

- Specificaţi dacă arhivaţi referinţe pentru dumneavoastră sau pentru toţi utilizatorii sistemului.
- Furnizaţi autentificarea hardware-ului de securitate prin introducerea parolei de sistem (pre-Windows), a parolei de administrator ControlVault şi a parolei de proprietar TPM.
- Creaţi o parolă a copiei de rezervă a referinţei.
- Specificaţi o locaţie de arhivare, folosind butonul **Browse** . Locaţia de arhivare ar trebui să fie un suport amovibil, cum ar fi o unitate flash USB sau o unitate din reţea, pentru a beneficia de protecţie contra defectării hard disk-ului.

Note importante:
- Notaţi locaţia arhivei, pentru că utilizatorul va avea nevoie de aceste informaţii pentru a restabili informaţiile de referinţă.
- Notaţi parola copiei de rezervă a referinţei pentru a vă asigura că datele pot fi restabilite. Acest aspect este important, deoarece parola nu poate fi recuperată.
- Dacă nu cunoaşteţi parola de proprietar TPM, contactaţi administratorul de sistem sau consultaţi instrucţiunile de instalare pentru TPM-ul de pe computer.

Restabilire referinţe
Pentru a restabili referinţe, trebuie să faceţi următoarele:

- Specificaţi dacă restabiliţi referinţe pentru dumneavoastră sau pentru toţi utilizatorii sistemului.
- Localizaţi locaţia arhivei şi selectaţi fişierul arhivă.
- Introduceţi parola copiei de rezervă a referinţei care a fost creată când aţi configurat arhiva.
- Furnizaţi autentificarea hardware-ului de securitate prin introducerea parolei de sistem (pre-Windows), a parolei de administrator ControlVault şi a parolei de proprietar TPM.

NOTE:

- Dacă primiţi o eroare că restabilirea referinţei a eşuat, şi aţi încercat de mai multe ori să efectuaţi o restabilire, încercaţi restabilirea pentru un fişier arhivă diferit. Dacă nu aţi reuşit, creaţi o altă arhivă de referinţe şi încercaţi restabilirea din noua arhivă.
- Dacă primiţi eroare prin care cheile TMP nu au putu fi restabilite, creaţi o arhivă de referinţe, apoi ştergeţi TPM în BIOS. Pentru ştergeţi TMP-ul, reporniţi computerul, apăsaţi tasta **F2**când începeţi realizarea copiei de rezervă pentru a accesa setările BIOS, apoi navigaţi până la Securitate>TPM Securitate. Apoi restabiliţi proprietatea TPM şi încercaţi să restabiliţi din nou referinţele.
- Pentru informaţii mai detaliate despre un anumit mesaj de eroare, accesaţi wave.com/support/Dell.

Gestionare parole

Din fereastra Gestionare parole, un administrator poate crea sau modifica toate parolele de securitate ale sistemului:

- Sistem (cunoscut drept Pre-Windows)*
- Administrator*
- Hard disk*
- ControlVault
- TPM Proprietar
- TPM Principal
- TPM Seif de parole
- Unitate cu autocriptare

NOTE:

- Se vor afişa doar acele parole care se folosesc pentru configuraţia curentă a platformei; drept urmare, această fereastră se va modifica în funcţie de configuraţia şi starea sistemului.
- Parolele de mai sus marcate cu * sunt parole BIOS şi pot fi modificate şi prin sistemul BIOS.
- Parolele la nivel de BIOS nu pot fi create sau modificate dacă administratorul BIOS administrator a interzis schimbările de parolă.
- Făcând clic pe link-ul**configurare** pentru o unitate cu autocriptare, se lansează aplicaţia de configurare a unităţii cu autocriptare; făcând clic pe **gestionare** utilizatorul poate modifica una sau mai multe parole ale unităţii cu autocriptare.
- Dacă faceţi clic pe link-ul **gestionare** pentru seiful de parole TPM, se afişează o fereastră în care puteţi vizualiza parolele care protejează cheile dumneavoastră TPM. Când este creată o cheie TPM care necesită o parolă, parola este generată aleatoriu şi plasată în seif. Nu puteţi gestiona seiful de parole TPM până nu aţi creat o parolă principală TPM.

Reguli de complexitate ale parolelor Windows

Dell Data Protection | Access se asigură că următoarele parole se conformează regulilor de de complexitate ale parolelor pentru computer:

- Parolăproprietar TPM

Pentru a determina politica de complexitate a parolelor Windows pentru un computer, urmaţi aceşti paşi:

1. Accesaţi Control Panel (panoul de comandă).
2. Faceţi dublu-clic pe Administrative Tools (instrumente administrative).
3. Faceţi dublu-clic pe Local Security Policy (Politica de securitate locală).
4. Desfăşuraţi Account Policies (Politici cont) şi selectaţi Password Policy (Politica de parole).

Dispozitive

Fereastra Dispozitive este folosită de administratori pentru a gestiona toate dispozitivele de securitate instalate pe sistemele lor. Pentru orice dispozitiv, puteţi vedea starea şi informaţii detaliate suplimentare, cum ar fi versiunea softului integrat. Faceţi clic pe **afişează** pentru a vizualiza informaţii despre fiecare dispozitiv, sau **ascunde** pentru a închide acea secţiune. Dispozitivele care pot fi gestionate sunt următoarele, în funcţie de care este platforma dumneavoastră:

Trusted Platform Module (TPM)
ControlVault®
Unitate (unităţi) cu autocriptare
Informaţii dispozitive de autentificare

Trusted Platform Module (TPM)

Cipul de securitate TPM trebuie să fie activat şi trebuie determinată proprietatea TPM pentru a folosi funcţiile de securitate avansate cu**Dell Data Protection | Access** şi TPM.

Fereastra Trusted Platform Module din **Gestionare unitate** este afişată doar când un TPM este detectat pe sistem.

Gestionare TPM

Aceste funcţii permit administratorului unităţii să gestionezeTPM-ul.

Stare
Afişează o stare de *activ* sau *inactiv* pentru TPM. Starea de"Activ" înseamnă că TPM-ul a fost identificat în sistemul BIOS şi este pregătit să fie configurat (adică, se poate prelua propietatea). TPM-ul nu poate fi gestionat şi funcţiile sale de securitate nu pot fi accesate dacă TPM-ul nu este activ (activat).

Dacă TPM-ul este detectat în sistem, dar nu este activ (activat), îl puteţi activa făcând clic pe linkul **activare** din fereastră, fără a intra în sistemul BIOS. După activarea TPM folosind această funcţie, computerul trebuie repornit. În timpul repornirii, este posibil să apară un mesaj prin care vi se cere să acceptaţi modificările.

NOTĂ: Posibilitatea de a activa TPM-ul din această aplicaţi nu este compatibilă cu toate platformele. Dacă nu este compatibilă, trebuie să o activaţi din sistemul BIOS. Pentru aceasta, reporniţi sistemul, apăsaţi tasta **F2** înainte ca Windows să se încarce pentru a intra în setările BIOS, apoi navigaţi la Securitate>TPM Securitate şi activaţi TPM-ul.

De asemena, puteţi *dezactiva* TPM-ul de aici făcând clic pe linkul **dezactivare**; prin dezactivare, TPM-ul devine indisponibil pentru funcţiile de securitate avansate. Totuşi, dezactivarea nu modifică niciuna din setările TPM-ului şi nu şterge sau modifică nici una din informaţiile sau cheile stocate în TPM.

Cu proprietar
Afişează starea de proprietate (adică "având proprietar") şi vă permite să stabiliţi sau să modificaţi proprietarul TPM. Proprietatea TPM trebuie stabilită pentu ca funcţiile sale de securitate să fie disponibile. Înainte ca proprietatea să poată fi stabilită, TPM-ul trebuie activat.

Procesul de stabilire a proprietăţii constă în crearea de către utilizator(cu drepturi de administrator) a unei parole de proprietar TPM. Odată definită această parolă, proprietarul este stabilit, iar TPM este gata de utilizare.

NOTĂ: parola de proprietar TPM trebuie se conformeze la Regulile de complexitate ale parolelor Windows pentru sistem.

Important! Este important să nu pierdeţi sau să uitaţi parola de proprietar TPM, şi este necesar pentru a accesa funcţiile de securitate avansate pentur TPM din **Dell Data Protection | Access**.

Blocat
Afişează o stare de *blocat* sau *deblocat* pentruTPM. "Blocarea" este o funcţie de securitate a TPM; TPM-ul va fi blocat după un anumit număr de încercări incorecte de introducere a parolei de proprietar TPM. Proprietarul TPM poate debloca TPM-ul de aici; este necesară introducera parolei de proprietar TPM.

NOTE:

- Dacă primiţi o eroare că proprietatea TPM-ului nu a putut fi stabilită, ştergeţi TPM-ul din sistemul BIOS şi încercaţi să stabiliţi proprietatea încă o dată. Pentru a şterge TPM-ul, reporniţi computerul, apăsaţi tasta **F2** la pornirea copiei de rezervă pentru a accesa setările BIOS, apoi navigaţi la Securitate>TPM Securitate.
- Dacă primiţi o eroare că parola de proprietar nu a putut fi schimbată,arhivaţi datele TPM (arhiva de referinţe), ştergeţi TPM-ul din BIOS, restabiliţi proprietatea TPM şi restabiliţi datele TPM (restabilire referinţe).
- Pentru informaţii mai detaliate despre un anumit mesaj de eroare, accesaţi wave.com/support/Dell.

Dell ControlVault®

Dell ControlVault® (CV) este un hardware de stocare securizat pentru referinţe de utilizator folosite în timpul autentificării pre-Windows (de ex., parole de utilizator sau date legate de amprente înregistrate). Fereastra ControlVault din **Gestiune dispozitive** este afişată doar când ControlVault este detectat pe sistemul dumneavoastră.

Gestiune ControlVault

Aceste funcţii permite administratorului de sistem să gestioneze ControlVault al sistemului.

Stare
Afişează starea de*activ* sau *inactiv* pentru ControlVault. Starea "Inactivă" înseamnă că ControlVault nu este disponibil pentru stocare pe sistemul dumneavoastră. Consultaţi documentaţia sistemului Dell pentru a determina dacă sistemul conţine un ControlVault.

Parola
Indică dacă parola de administrator ControlVault a fost configurată, şi vă permite să configuraţi o parolă sau să modificaţi parola (dacă există deja una configurată). Doar administratorii de sistem pot configura sau modifica această parolă. O parolă de administrator ControlVault trebuie să fie configurată pentru a efectua următoarele:

- Efectuarea unei arhivări sau restabiliri de referinţe.
- Ştergerea datelor de utilizatori (pentru toţi utilizatorii).

NOTĂ: Dacă se încearcă o arhivare sau o restabilire cât timp parola de administrator ControlVault nu a fost configurată, utilizatorului i se va solicita să creeze una nouă (dacă este administrator).

Utilizatori înregistraţi
Indică dacă un utilizator a înregistrat referinţe de autentificare (de ex..date referitoare la parole, amprente sau smartcard) care sunt stocate curent în ControlVault.

Ştergere date utilizator
Datele din ControlVault vor trebui să fie şterse la un moment dat; de exemplu, dacă utilizatorii au probleme în folosirea sau înregistrarea de referinţe pre-Windows pentru autentificare. Toate datele stocate în ControlVault pot fi şterse, pentru un singur utilizator sau pentru toţi, din această fereastră.

Trebuie introdusă parola de administrator ControlVault pentru a şterge toate datele de utilizator de pe platformă. De asemenea, vi se va solicita parola de sistem (pre-Windows) dacă sunt înregistrate orice referinţe pre-Windows. Când ştergeţi toate datele de utilizator, parola de administrator ControlVault şi parola de sistem sunt resetate; reţineţi că aceasta este singura modalitate de a şterge parola de administrator ControlVault.

NOTĂ: După ce aţi şters toate datele de utilizator, vi se va solicita să reporniţi computerul. Este important să reporniţi computerul pentru funcţionarea corectă a sistemului dumneavoastră.

Parola de administrator ControlVault nu trebuie configurată pentru a şterge referinţele unui singur utilizator. Când faceţi clic pe **ştergere date de utilizator**, vi se va solicita să selectaţi utilizatorul ale cărui referinţe ControlVault doriţi să le ştergeţi. După ce aţi selectat un utilizator, vi se va solicita parola de sistem (doar dacă sunt înregistrate referinţe pre-Windows).

NOTE:

- Dacă primiţi o eroare că parola de administrator ControlVault Administrator nu poate fi creată, e indicat să vă arhivaţi referinţele, să ştergeţi toate datele de utilizator din ControlVault, să reporniţi computerul şi să încercaţi parola din nou.
- Dacă primiţi o eroare că referinţele nu pot fi şterse din ControlVault pentru un singur utilizator, e indicat să vă arhivaţi referinţele, să încercaţi să ştergeţi toate datele de utilizator şi apoi să încercaţi să ştergeţi datele acelui utilizator încă o dată.
- Dacă primiţi o eroare că referinţele nu au putut fi şterse din ControlVault pentru toţi utilizatorii, e indicat să efectuaţi o resetare de sistem. **Important!** Revedeţi subiectul de ajutor Resetare sistem înainte de efectuarea resetării, deoarece acest lucru va şterge TOATE datele de utilizator securizate.
- Dacă primiţi o eroare că pentru datele ControlVault şi TPM nu s-a putut realiza o copie de rezervă, dezactivaţi TPM-ul din sistemulBIOS. Acest lucru se face repornind computerului, apăsând pe butonul **F2** când începeţi realizarea copiei de rezervă pentru a accesa setările BIOS, apoi navigând la Securitate >TPM Securitate. Apoi reactivaţi TPM-ul şi încercaţi din nou să vă arhivaţi datele ControlVault.
- Pentru informaţii mai detaliate despre un anumit mesaj de eroare, accesaţi wave.com/support/Dell.

Unităţi cu autocriptare: Configurare avansată

Dell Data Protection | Access gestionează funcţiile de securitate bazate pe hardware al unităţilor cu autocriptare, care au au încorporat în unitatea hardware funcţia de criptare a datelor. Prin această gestionare se asigură că doar utilizatorii autorizaţi pot accesa datele criptate atunci când este activată blocarea unităţii.

Fereastra Unitate cu autocriptare din **Gestionare dispozitive** este afişată doar când una sau mai multe unităţi cu autocriptare (SED) sunt prezente în sistem.

Important! După ce unitatea cu autocriptare a fost configurată, sunt "activate" protecţia datelor de pe unitatea cu autocriptare şi blocarea unităţii.

Gestionare unitate
Aceste funcţii permit administratorului unităţii să gestioneze setările desecuritate ale unităţii. Modificările setărilor de securitate ale unităţii se aplică după ce unitatea a fost oprită.

Protecţia datelor
Afişează starea de *activat* sau *dezactivat* pentru protecţia datelor de pe unitatea cu autocriptare. Starea "activat" înseamnă că securitatea unităţii a fost configurată; totuşi, până când *blocarea* unităţii este aprinsă, utilizatorii nu vor trebui să se autentifice pe unitate la accesul pre-Windows.

Puteţi dezactiva protecţia datelor de pe unitatea de autocriptare de aici. Când este dezactivată, toate funcţiile de securitate avansate ale unităţii cu autocriptare sunt stinse şi unitatea acţionează ca o unitate standard. Dezactivarea protecţiei datelor şterge şi toate setările de securitate, inclusiv referinţele administratorului unităţii şi ale utilizatorilor unităţii. Această funcţie, totuşi, nu modifică şi nu şterge nicio dată a utilizatorilor de pe unitate.

Blocare
Afişează o stare de *activat* sau *dezactivat* pentru unitatea(unităţile) cu autocriptare. Consultaţi subiectul Unitate cu autocriptare pentru informaţii despre comportamentul unităţii blocate.

Poate fi necesară dezactivarea temporară a blocării unităţii, lucru pe care îl puteţi face de acasă. Acest lucru nu este recomandat deoarece nu sunt necesare referinţe pentru a accesa unitatea când blocarea unităţii este dezactivată, astfel că orice utilizator de platformă poate accesa datele unităţii. Dezactivarea blocării unităţii nuşterge oricare din setările de securitate, inclusiv referinţele pentru administratorul unităţii şi utilizatorii unităţii, sau orice utilizator de date de pe unitate.

ATENŢIE!Dacă dezinstalaţi aplicaţia **Dell Data Protection | Access**, întâi trebuie să dezactivaţi protecţia datelor de pe unitatea cu autocriptare şi să deblocaţi unitatea.

Administrator unitate

Afişează administratorul curent al unităţii. Administratorul de unitate poate modifica de aici care utilizator este administratorul unităţii. Noul administrator trebuie să fie un utilizator Windows valid pe sistem cu drepturi de administrator. Pe sistem poate fi doar un singur administrator al unităţii.

Utilizatorii unităţii

Afişează utilizatorii înregistraţi ai unităţii şi numărul utilizatorilor înregistraţi actual. Numărul maxim de utilizatori acceptaţi este în funcţie de unitatea cu autocriptare (în prezent, 4 utilizatori pentru unităţi Seagate şi 24 pentru unităţi Samsung).

Parola Windows Sincronizare
Funcţia de sincronizare a parolelor Windows (WPS) setează în mod automat ca parolele utilizatorilor unităţii cu autocriptare să fie identice cu parolele Windows ale acestora. Această funcţie nu se aplică administratorului de unitate, ci doar utilizatorilor unităţii. Funcţia WPS poate fi folosită în medii organizaţionale în care parolele trebuie schimbate la anumit intervale de timp (de ex., la fiecare 90 de zile); când această opţiune este activată, toate parolele utilizatorilor unităţii cu autocriptare vor fi actualizate în mod automat când aceste parole Windows vor fi schimbate

NOTĂ: Când sincronizarea parolelor Windows (WPS) este activată, parola unui utilizator al unităţii cu autocriptare nu poate fi modificată; parola Windows a acestora trebuie modificată pentru a actualiza în mod automat parola de unitate.

Reţineţi ultimul nume de utilizator
Când această opţiune este activată, ultimul nume de utilizator introdus va fi afişat în mod implicit în câmpul **Nume de utilizator** pe ecranul de autentificare pre-Windows.

SelectareNume de utilizator
Când această opţiune este activată, utilizatorii pot vizualiza toate numele de utilizator ale unităţii în câmpul **Nume de utilizator**pe ecranul de autentificare pre-Windows.

Ştergerecriptografică
Această opţiune poate fi folosită pentru a "şterge" toate datele de pe unitatea cu autocriptare. Această acţiune nu şterge efectiv datele, dar şterge cheile folosite pentru criptarea datelor, şi prin aceasta, face datele nefolosibile. După ştergerea criptografică, datele de pe unitate nu se mai poţi recupera; de asemenea, este dezactivată protecţia datelor de pe unitatea cu autocriptare şi unitatea este gata să fie pregătită pentru folosirea în alt scop.

NOTE:
- Dacă primiţi orice tip de erori referitoare la funcţiile gestionării unităţii cu autocriptare, stingeţi complet computerul (nu o repornire), şi restartaţi-l.
- Pentru informaţii mai detaliate despre un anumit mesaj de eroare, accesaţi wave.com/support/Dell.

Informaţii dispozitive de autentificare

Fereastra Informaţii dispozitive de autentificare din **Gestionare dispozitiv** afişează informaţii şi starea tuturor dispozitivelor de autentificare conectate la sistem (adică cititor de amprente, cititor de smartcard tradiţional sau contactless).

Asistenţă tehnică

Asistenţa tehnică pentru software-ul **Protecţia datelor Dell | Accesare** se găseşte la http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP

Furnizorul de servicii criptografice (CSP) compatibil Wave Systems Trusted Computing Group (TCG) este inclus în aplicaţia **Dell Data Protection | Access** , şi este disponibil pentru utilizare ori de câte ori este necesar un furnizor de servicii criptografice (CSP) – fie apelat direct dintr-o aplicaţie, fie selectabil dintr-o listă de CSP-uri instalate. Când este posibil, selectaţi “Wave TCG-Enabled CSP” pentru a vă asigura că TPM generează cheile şi că aceste chei şi parolele lor sunt gestionate de **Dell Data Protection | Access**.

Wave Systems TCG-enabled CSP permite aplicaţiilor să utilizeze funcţiile disponibile pe platformele compatibile TCG direct prin MSCAPI. Este un modul CSP MSCAPI cu supliment TCG care oferă funcţionalitate de chei asimetrice pe TPM şi sporeşte securitatea suplimentară oferită de TPM, indiferent de cerinţele specifice fabricantului cu privire la furnizorul de stivă software Trusted (TSS).

NOTĂ: În cazul în care cheile TPM generate de Wave TCG-enabled CSP solicită o parolă şi utilizatorul a creat o parolă principală TPM, parolele individuale ale cheilor vor fi generate aleatoriu şi stocate în TPM Password Vault.