Dell Data Protection | Access Home

Dell Data Protection | Access domača stran je izhodišče za dostop do funkcij te aplikacije. Iz tega okna lahko dostopate do naslednjega:

System Access Wizard
Možnosti dostopa
Self-Encrypting Drive
Dodatne možnosti

V spodnjem desnem kotu okna je povezava z imenom **dodatno**, ki lahko kliknete za dostop do dodatnih možnosti.

Iz polja dodatne možnosti, lahko kliknete povezavo **domov** v spodnjem desnem kotu okna in se tako vrnete na domačo stran.

System Access Wizard

System Access Wizard se samodejno zažene prvič, ko se začne uporaba aplikacije **Dell Data Protection | Access**. Ta čarovnik vas vodi skozi nastavljanje vseh vidikov varnosti vašega sistema, vključno s tem, kako (na primer samega gesla ali prstnega odtisa in gesla) in kdaj se želite prijaviti v sistem (v Windows, pre-Windows ali oboje). Poleg tega, če ima vaš sistem samo-šifrirni pogon, ga lahko nastavite s pomočjo tega čarovnika.

Skrbniške funkcije

Uporabniki, ki so bili nastavljeni z WIndows pravicami skrbnika, imajo v sistemu pravice do opravljajo naslednje naloge v **Dell Data Access | Protection**, ki je standardni uporabniki ne morejo:

- Nastavljanje / sprememba sistemskega (Pre-Windows) gesla
- Nastavljanje / sprememba gesla trdega diska
- Nastavljanje / sprememba gesla skrbnika
- Nastavitev / sprememba gesla lastnika TPM
- Nastavljanje / sprememba gesla ControlVault skrbnika
- Ponovni zagon sistema
- Arhiviraj in obnovi akreditive
- Nastavljanje / sprememba PIN-a smartcard skrbnika
- Zbris / reset smartcard
- Omogoči / onemogoči Dell varno prijavo v Windows
- Nastavitev Windows prijavnih pravil
- Upravljanje samo-šifrirnih pogonov, vključno z:
    - Omogoči / onemogoči zaklepanje samo-šifrirnega pogona
    - Omogoči / onemogoči Windows Password Synchronization (WPS)
    - Omogoči / onemogoči Single Sign On (SSO)
    - Opravljanje kriptografskega izbrisa

Upravljanje na daljavo

Vaša organizacija lahko vzpostavi okolje, v katerem se varnostne funkcije aplikacij **Dell Data Protection | Access** na več platformah centralno upravljajo (npr. daljinsko upravljanje). V tem primeru se Windows varnostna infrastruktura, kot je Active Directory, uporablja za varno upravljanje posebnosti **Dell Data Protection | Access**.

Ko je računalnik daljinsko upravljan (npr. "v lasti" s strani oddaljenega skrbnika), bo lokalni skrbnik za **Dell Data Protection | Access** funkcionalnost onemogočen; upravljalno okno aplikacije pa lokalno ne bo dostopno. Upravljanje naslednjih funkcij je mogoče izvajati daljinsko:

- Trusted Platform Module (TPM)
- ControlVault
- Pre-Windows prijava
- Ponovni zagon sistema
- BIOS gesla
- Windows pravila prijave
- Self-Encrypting Drives
- Vpis preko prstnih odtisov in Smartcard-a

Za več informacij o uporabi Wave Systems "EMBASSY® Remote Administration Server (ERAS) za daljinsko upravljanje, se obrnite na Dell prodajalca ali obiščite dell.com.

Možnosti dostopa

V oknu Možnosti dostopa lahko nastavite, kako boste imeli dostop do vašega sistema.

Če imate nastavljene **Dell Data Protection | Access** možnosti, bodo te prikazane na domači strani z razpoložljivimi možnostmi (npr., spremenite geslo za prijavo v pre-Windows). Razpoložljive možnosti so bližnjice, ki vas ob kliku vodijo do ustreznega okna za opravljanje posebne naloge (npr. sprememba vašega gesla za prijavo v pre-Windows ali za registriranje drugih prstnih odtisov).

Splošno
Prvič, določite, lahko kdaj se prijavite (Windows, pre-Windows ali oboje) in kako se prijaviti (na primer s prstnimi odtisi in geslom). Izbirate lahko med eno ali dvema možnostmi, kako se boste prijavili, kar vsebuje kombinacije prstnih odtisov, pametne kartice in gesla. Naštete možnosti so v vašem okolju aplicirane na podlagi prijavnih pravil in temu, kaj je podprto na platformi.

Prstni odtis
Če vaš sistem vsebuje čitalec prstnih odtisov, lahko vnesete ali posodobite prstne odtise za uporabo pri prijavi v vaš sistem. Ko ste enkrat vnesli prstne odtise, lahko povlecete s vpisanih prstom ali prsti po vašem sistemskem čitalcu prstnih odtisov za dostop do vašega sistema na Windows, pre-Windows ali oboje (odvisno, kaj ste določili v področju Splošne možnostih za dostop). Za več informacij poglejte Vnos prstnih odtisov uporabnika.

Prijava pre-Windows
Če ste določili, da morajo biti uporabniki prijavljeni v pre-Windows, morate za dostop do pre-Windows vzpostaviti sistemsko geslo (včasih imenovano pre-Windows geslo). Ko je to nastavljeno, lahko skrbnik v vsakem trenutku spremeni geslo.

Lahko tudi s tega zaslona onemogočite prijavo v pre-Windows; zato morate vnesti svoje trenutno sistemsko geslo, preveriti ali je geslo pravilno, nato klikniti gumb **Onemogoči**.

Smartcard
Če ste določili, da morajo uporabniki za prijavo uporabljati pametne kartice, morate vpisati eno ali več tradicionalnih (kontaktnih) ali brezkontaktnih pametnih kartic. Kliknite povezavo **Vnesi drugo smartcard**, da zaženete čarovnika za vpis pametne kartice. Vpis pomeni nastavitev vaše pametne kartice za uporabo v prijavi.

Ko ste enkrat vpisali pametno kartico, lahko spremenite ali nastavite PIN za to kartico z uporabo povezave**Spremeni ali nastavi moj smartcard PIN**.

Prijava v Pre-Windows

Ko je prijava v pre-Windows nastavljena, morate zagotoviti preverjanje pristnosti (geslo, prstni odtis ali pametno kartico), ko je sistem v teku, preden se naloži operacijski sistem Windows. Prijavna Pre-Windows funkcionalnost zagotavlja dodatno varnost za sistem, kar preprečuje nepooblaščenim uporabnikom ogrožanje Windows-a in dostop do računalnika (npr., ko je bil ukraden).

Iz okna Pre-Windows prijava, lahko skrbniki nastavljajo prijavo v pre-Windows, ustvarijo ali spremenijo pre-Windows (sistemsko) geslo; če je to geslo že bilo vzpostavljeno, lahko s tega okna onemogočite prijavo v pre-Windows. Nastavitev prijave v pre-Windows bo zagnala čarovnik, ki bo naredil naslednje:

- Sistemsko geslo: Vzpostavitev sistemskega gesla (imenovano tudi pre-Windows geslo) za pre-Windows dostop. To geslo se uporablja tudi kot varnostno kopiranje v primerih, v katerih ima uporabnik dodatne dejavnike preverjanje pristnosti (npr. dostop do sistema, če je težava s senzorjem prstnih odtisov).
- Prtsni odtis ali Smartcard: Vzpostavljanje prstnega odtisa ali pametne kartice za uporabo pri prijavi v pre-Windows, ter določitev ali bo ta overitveni faktor uporabljen namesto ali dodatno k pre-Windows geslu.
- Single Sign On: Privzeto se bo vaše pre-Windows preverjanje pristnosti (geslo, prstni odtis ali pametna kartica) uporabilo, da vas samodejno prijavi v Windows, kot se to tudi imenuje "Enkratni vpis". Za izklop te funkcije, izberite potrditveno polje "Želim se ponovno prijaviti v Windows".
- Če je BIOS geslo trdega diska bilo določeno poleg gesla za pre-Windows, boste imeli tudi možnost, da spremenite ali onemogočite geslo trdega diska.

OPOMBA: Niso vsi čitalci prstnih odtisov omogočeni za uporabo pre-Windows overjanje. Če vaš čitalec ni združljiv, morda ne boste mogli vnesti prstnih odtisov za prijavo edino v Windows. Če želite izvedeti ali je določena naprava združljiva, se obrnite na skrbnika sistema ali pa pojdite na support.dell.com, kjer je seznam podprtih čitalcev prstnih odtisov.

Onemogočanje Prijave Pre-Windows
S tega okna lahko tudi onemogočite prijavo v pre-Windows, za to boste morali vnesti svoje trenutno pre-Windows (sistemsko) geslo; preverite, ali je geslo pravilno in nato kliknite gumb **Onemogoči**. Upoštevajte, da če onemogočite prijavo v pre-Windows, ostanejo katero koli prstni odtisi ali pametne kartice vpisane.

Vnos prstni odtisov

Uporabniki lahko registrirajo ali posodobijo , ki se lahko uporabljajo za preverjanje pristnosti v sistemu bodisi za prijavo v pre-Windows ali v sam Windows. Na zavihku Prstni odtis, slike rok prikažejo, če in kateri prsti so bili vnešeni. S klikom na povezavo**Vnesi novega**, zaženete Fingerprint Enrollment wizard, ki vas vodi skozi postopek vnosa. "Vnos" pomeni shranjevanje prstnega odtisa, ki se uporablja za prijavo. Imeti morate pravilno nameščen in nastavljen čitalec prstnih odtisov, da se lahko vnaša prstne odtise.

OPOMBA: Ne morejo se uporabljati vsi čitalci prstnih odtisov za prijavo v pre-Windows. Sporočilo o napaki se bo prikazalo, če boste poskušali vnesti nezdružljivi čitalec za pre-Windows. Če želite izvedeti ali je naprava združljiva, se obrnite na skrbnika sistema ali pa pojdite na support.dell.com, kjer je seznam podprtih čitalcev prstnih odtisov.

Ko vnesete prstni odtis, boste morali vnesti geslo za Windows, da preveri vašo identiteto. Če vaša pravila zahtevajo, boste morali vnesti tudi vašo Pre-Windows (sistemsko) geslo. Pre-Windows geslo se lahko uporablja za dostop do sistema, če obstaja težava s čitalcem prstnih odtisov.

OPOMBE:

- Priporočljivo je, da ste vnesli vsaj dva prstna odtisa v postopku vnosa.
- Zagotoviti morate, da so prstni odtisi pravilno vnešeni, preden omogočite preverjanje pristnosti prstnih odtisov.
- Če na sistemu spremenite čitalec prstnih odtisov, morate ponovno vnesti prstne odtise z novim čitalcem. Preklapljanje med dvema različnima čitalcema prstnih odtisov ni priporočljivo.
- Če se ponavlja prikazano sporočilo "senzor je izgubil focus", ko vnašate prstne odtise, to lahko pomeni, da računalnik ni prepoznal čitalca prstnih odtisov. Če je čitalec prstnih odtisov zunanji, ga odklopite in ponovno priklopite in to največkrat odpravi težavo.

Brisanje vnešenih prstnih odtisov
Odstranite lahko vnešene prstne odtise s klikom na povezavo **Odstrani prstne odtise** ali s klikom na (za odznačitev) vnešenega prsta v čarovniku prstnih odtisov.

Če želite odstraniti določenega uporabnika, ki ima vnešene prstne odtise za preverjanje pristnosti v pre-Windows, lahko skrbnik odznači vse prstne odtise, ki so vnešeni za tega uporabnika.

OPOMBA: Če se pojavijo morebitne napake med postopkom vnosa prstnih odtisov, se lahko obrnete za dodatne podrobnosti na wave.com/support/Dell.

Vnos SmartCard

Dell Data Protection | Access vam daje možnost uporabe običajne (kontaktne) ali brezkontaktne pametne kartice za prijavo v vaš račun Windows ali preverjanje overjanja v pre-Windows-u. V Smartcard jezičku, kliknite povezavo **Vnesi novo smartcard**, da zaženete Smartcard Enrollment wizard, ki vas vodi skozi postopek vnosa. "Vnos" pomeni nastavitev vaše pametne kartice za uporabo v prijavi.

Za opravljanje vnosa morate imeti pravilno nameščeno in nastavljeno veljavno napravo za preverjanje pristnosti pametne kartice.

OPOMBA: Če želite izvedeti ali je dotična naprava združljiva, se obrnite na skrbnika sistema ali pa poglejte na support.dell.com seznam podprtih pametnih kartic.

Vnos
Ko vnesete pametno kartico, boste morali vnesti geslo za Windows, da preveri vašo identiteto. Če vaša pravila zahtevajo, boste morali vnesti tudi vašo pre-Windows (sistemsko) geslo. Pre-Windows geslo se lahko uporablja za dostop do sistema, če je težava z čitalcem pametne kartice.

Med vnosom boste morali vnesti PIN za pametno kartico, če je bil ta določen. Če vaša pravila zahtevajo PIN in še nihče ni bil določen, boste pozvani, da eno ustvarite.

OPOMBE:

- Ko je enkrat vnešen uporabnik za uporabo pametne kartice v pre-Windows, tega ni mogoče več odstraniti.
- Standardni uporabniki lahko spremenijo uporabniški PIN na pametni kartici, in skrbnik lahko spremeni oba, skrbniški PIN in uporabniški PIN.
- Srkbnik lahko tudi ponastavi pametno kartico; ko je enkrat ponastavljena, pametne kartice ni mogoče uporabiti za preverjanje pristnosti ob prijavi v Windows ali pre-Windows, dokler ni ponovno vnešena.

OPOMBA: Za preverjanje pristnosti potrdila TPM, lahko skrbniki vpišejo TPM potrdila preko Microsoft Windows postopka vnosa pametne kartice. Skrbniki morajo izbrati "Wave TCG-Enabled CSP" kot Cryptographic Service Provider namesto Smartcard CSP za združljivost s to aplikacijo. Poleg tega mora biti omogočena Dell Secure prijava z ustreznimi za stranko Authentication Type Policy.

OPOMBA: Če se pojavi napaka, ki navaja, da Smartcard Service ne deluje, lahko zaženete / ponovno zaženete to storitev tako, da naredite naslednje:

- Pojdite v okno Administrativna orodja pod Nadzorna plošča, izberite Storitve, nato z desno tipko miške kliknite na pametno kartico in izberite Start ali Ponovni zagon.
- Če želite podrobnejše informacije o določenem sporočilu o napaki, pojdite na wave.com/support/Dell.

Self-Encrypting Drive

Dell Data Protection | Access upravlja na osnovi strojne opreme z varnostnimi funkcijami samo-šifrirnih pogonov, ki imajo šifriranje podatkov vključeno v pogon strojne opreme. Ta funkcija se uporablja za zagotovitev, da lahko imajo dostop le pooblaščeni uporabniki šifriranih podatkov (ko je omogočeno zaklepanje pogona).

Do okna Self-Encrypting Drive dostopate s klikom na spodnji zavihek **Self-Encrypting Drive**. Ta zavihek se prikaže le, ko je prisotnih na vašem sistemu eden ali več samo-šifriranih pogonov (SEDs).

Kliknite povezavo **Nastavitve**, da zaženete Self-Encrypting Drive namestitveni čarovnik. V tem čarovniku, boste ustvarili geslo skrbnika pogona, varnostno shranili to geslo in nato uporabili nastavitve šifriranja pogona. Samo skrbniki sistema lahko dostopajo do Self-Encrypting Drive namestitvenega čarovnika.

Pomembno! Ko je pogon nastavljen, je "omogočeno" varovanje podatkov in zaklepanje pogona. Ko je pogon zaklenjen, velja naslednje:

- Pogon preide v *zaklenjen*način, kadarkoli se izklopi napajanje pogona.
- Pogon se ne bo ponovno zagnal razen, če uporabnik vnese pravilno uporabniško ime in geslo (ali prstni odtis) v zaslonu prijave v Pre-Windows. Preden je omogočeno zaklepanje pogona, so podatki na pogonu na voljo vsem uporabnikom na računalniku.
- Pogon je zavarovan, tudi če je priključen na drug računalnik kot sekundarni disk, preverjanje pristnosti je potrebno za dostop do podatkov pogona.

Ko je pogon nastavljen, bo okno Self-Encrypting Drive prikazalo disk(e) in povezavo za uporabnike za spremembo njihovih gesel pogona. Če ste skrbnik pogona, boste prav tako s tega okna lahko dodajali ali odstranjevali uporabnike pogona. Če je tukaj zunanji disk, ki je bil nastavljen, se bo prikazal v tem oknu in se bo lahko odklenil.

OPOMBA: Če želite zakleniti sekundarni, zunanji disk, se mora pogon izklopiti neodvisno od računalnika.

Skrbnik pogona lahko upravlja nastavitve pogona v **Dodatno>Naprave**. Za več informacij, glejte Device Management - Self-Encrypting Drives.

Nastavitev pogona

Self-Encrypting Drive čarovnik namestitve vas bo vodil skozi nastavitev vašega diska ali diskov. Ko gremo skozi ta proces je pomembno imeti v mislih naslednje pojme.

PogonSkrbnik
Prvi uporabnik s pravicami skrbnika sistema, ki nastavlja dostop do pogona (in nastavlja geslo skrbnika pogona) postane skrbnik pogona, to je edini uporabnik s pravicami do sprememb dostopa do pogona. Da bi zagotovili, da je bil prvi uporabnik namerno nastavljen kot skrbnik pogona, morate za nadaljevanje tega koraka izbrati polje "Razumem".

Skrbnik pogonaGeslo
Čarovnik vas bo pozval, da ustvarite geslo skrbnika pogona ter ga nato ponovno vnesete za potrditev. Vnesti morate svoje geslo za Windows, da vzpostavite vašo identiteto, preden lahko ustvarite geslo skrbnika pogona. Trenutni Windows uporabnik mora imeti skrbniške pravice za ustvarjanje tega gesla.

Poverilnice za pogon varnostne kopije
Vnesite v lokacijo ali kliknite gumb **Poišči** in izberite mesto, da shranite varnostno kopijo vaše poverilnice skrbnika pogona.

POMEMBNO**!**

- Zelo je priporočljivo, da ustvarite varnostno kopijo teh poverilnic in da jih varnostno kopirate na pogon, ki ni vaš primarni trdi disk (npr. izmenljiv medij). V nasprotnem primeru, če izgubite dostop do vašega pogona, ne boste mogli dostopati do varnostne kopije.
- Ko zaključite nastavitev pogona, bo moral vsakuporabnik vnesti pravilno uporabniško ime in geslo (ali prstni odtis), preden se naloži Windows, da bi imel dostop do sistema, ko se naslednjič zaganja.

Dodaj uporabnika pogona
Skrbnik pogona lahko doda druge uporabnike pogona, ki veljajo za Windows uporabnike. Ko dodajate uporabnike za pogon, ima skrbnik možnost zahtevati od uporabnika, da ponastavi svoje geslo ob prvi prijavi. Uporabnik bo moral ponastaviti svoje geslo na zaslonu pre-Windows overjanja pristnosti, preden se bo pogon odklenil.

Napredne nastavitve

- *Single Sign On* - Glede na privzeto se bo vaše geslo Self-Encrypting Drive, ki ste ga vnesli v pre-Windows za preverjanje pristnosti pogona, samodejno uporabila za prijavo v Windows (to se imenuje "Single Sign On"). Za izklop te funkcije, izberite potrditev polja "Želim se ponovno prijaviti v Windows", kadar konfigurirate vaše nastavitve pogona.
- *Prijava s prstnim odtisom* - Na podprtih platformah lahko določite, da želite za overjanje na vaš self-encrypting drive uporabiti prstne odtise namesto gesla.
- *Spanje/Pripravljenost (S3) Podpora* (če je podprto na platformi) - Če je omogočeno, lahko vaš self-encrypting drive varno preide v stanje spanja / pripravljenosti (imenovan tudi S3 način) in bo zahteval pre-Windows preverjanje pristnosti, ko se bom povrnil iz spanja / stanja pripravljenosti.

OPOMBE:

- Ko je omogočena S3 podpora, se gesla šifrirnega pogona nanašajo na omejitve BIOS gesla, ki lahko obstajajo. Za dodatne informacije o posebnih omejitvah BIOS gesla, ki lahko obstaja za sistem, se posvetujte s proizvajalcem strojne opreme.
- Vsi samo-šifrirni pogoni ne podpirajo S3 način. Med nastavitvijo pogona, boste dobili sporočilo, če pogon podpira spanje / mirovanje. Za pogone, ki ne podpirajo ta način, bo Windows S3 zahteva avtomatično pretvorjena v zahtevo mirovanja, če je omogočen način mirovanja (zelo je priporočljivo, da ste omogočili način mirovanja na vašem računalniku). stanje mirovanja na vašem računalniku).
- Ko se prvič prijavite po nastavitvi Single Sign On (SSO) možnosti, se bo ob takojšnji prijavi v Windows proces zaustavil v pavzi. Za vstop boste morali izpolniti obrazec preverjanja pristnosti za Windows, ki bo varno shranjen za prihodnje poskuse prijave v Windows. Naslednjič, ko se bo sistem ponovno zaganjal, bo SSO samodejno izvedel prijavo v Windows. Isti postopek se zahteva tudi, kadar se bo uporabnikovo preverjanje pristnosti za Windows (geslo, prstni odtis, PIN pametne kartice) spremenilo. Če je računalnik v domeni, in ima domena pravila, ki zahtevajo za prijavo v Windows pritisk tipk ctrl+alt+del, bo ta pravila potrebno spoštovati.

POZOR! Če odstranite aplikacijo **Dell Data Protection | Access**, morate najprej onemogočiti self-encrypting drive zaščito podatkov in odklepanje pogona.

Self-Encrypting Drive uporabniške funkcije

Skrbniki Self-encrypting drive izvajajo vse, od upravljanja varnosti pogona do uporabnikov. Uporabniki pogonov, ki niso skrbniki, lahko izvajajo le naslednje naloge:

- Spremenijo geslo njihovega pogona
- Odklenejo pogon

Te naloge so dostopne v zavihku **Self-Encrypting Drive** v **Dell Data Protection | Access**.

Sprememba gesla
To omogoča vnešenim uporabnikom, da ustvarijo novo geslo za preverjanje pristnosti svojega pogona. Vpisati morate svoje trenutno Self-Encrypting Drive geslo, preden je geslo pogona nastavljeno na novo vrednost.

OPOMBE:

- Aplikacija bo zahtevala dolžino gesla za Windows in pravila kompleksnosti gesla, če so le-te omogočene. Če Windows pravila gesel niso omogočena, je največja dolžina gesla 32 znakov za Self-Encrypting Drive. Upoštevajte, da je največja dolžina 127 znakov, če ni omogočen S3 (Spanje/Pripravljenost).
- Uporabnikovo geslo za Self-Encrypting Drive je ločeno od njihovega gesla za Windows. Ko je uporabnikovo geslo za Windows spremenjeno ali ponastavljeno, to nima nobenega vpliva na geslo uporabnikovega pogona razen, če je bila omogočena Windows sinhronizacija gesel. Za detajle poglejte Devices: Self-Encrypting Drives.
- Na nekaterih ne-angleški tipkovnicah, obstaja določena skupina omejenih znakov, ki se ne morejo uporabljati za geslo samo-šifriranega pogona. Če geslo za Windows vsebuje katerega koli od omejenih znakov, in je omogočen Windows Password Synchronization, sinhronizacija ne bo uspela in bo nastalo sporočilo o napaki.

Odklenitev pogona
Odklenite pogona omogoča vnešenemu pogonu odklepanje zaklenjenega pogona . Če je omogočeno zaklepanje pogona, gre pogon v zaklenjeno stanje, kadar je računalnik izklopljen. Ko je sistem ponovno vklopljen, morate overiti pogon z vnosom gesla v zaslon pre-Windows overovljenja.

OPOMBE:

- Nezmožnost za prehod v način za varčevanje z energijo (npr. način spanja / stanja pripravljenosti ali mirovanja), se dogodi, če je več self-encrypting drive uporabniških računov hkrati aktivnih na računalniku.
- Na zaslonu pre-Windows overovitve se "Uporabnik1", "" Uporabnik2 ", itd. nadomestijo z imeni pogonov v različicah aplikacij, ki so lokalizirane za naslednje jezike: kitajski, japonski, korejski in ruski.

Dodatne možnosti

Dodatne možnosti v **Dell Data Protection | Access** omogočajo uporabniku s pravicami skrbnika, da lahko upravlja naslednje vidike aplikacije:

Vzdrževanje
Geslo
Naprave

OPOMBA Samo uporabniki s pravicami skrbnika lahko spremenijo Dodatne možnosti; običajni uporabniki lahko gledajo te nastavitve, vendar jih ne morejo spreminjati.

Vzdrževanje

Okno za Vzdrževanje lahko uporabljajo skrbniki za vzpostavitev Windows prijavnih nastavitev, ponastavitve sistema ali da ga pripravijo na spremembo namembnosti ali arhiviranje ali obnovtev uporabniških poverilnic shranjenih na strojni opremi varnostnega sistema. Za podrobnosti poglejte naslednje teme:

Preference dostopa
Ponovni zagon sistema
Credential Archive & Restore

Preference dostopa

Okno preference dostopa omogoča skrbnikom določiti Windows prijavne preference za vse uporabnike sistema.

OmogočiDell varnostno prijavo
Možnost za zamenjavo standardnega Windows zaslona s tipkami ctrl-alt-delete, vam omogoča uporabo različnih dejavnikov preverjanja pristnosti namesto (ali poleg) Window gesla za dostop do Windows-a. Če želite, lahko dodate prstnih odtis kot drugi dejavnik preverjanja pristnosti, da se okrepi varnost procesa prijave v Windows. Lahko se dodajo tudi dodatni dejavniki za preverjanje pristnosti prijave v Windows, vključno z elektronsko kartico ali TPM potrdilom.

OPOMBE:

- Omogočanje Dell varne prijave vpliva na vse uporabnike v sistemu.
- Priporočeno je, da je ta možnost omogočena ZA TEM, ko so uporabniki vnesli svoje prstne odtise ali pametne kartice.
- Ko se prvič prijavite po nastavitvi te možnosti, boste morali dokazati pristnost za Windows po vaših standardnih pravilih, nato pa boste morali pri naslednjem zagonu uporabiti vaš(e) nov(e) dejavnik(e) overjanj(a).

Onemogočanje Dell varnostne prijave
Ta možnost za prijavo v Windows onemogoči vse **Dell Data Protection | Access**funkcije. Ko je ta izbrana, se boste vrnili na vaša standardna Windows prijavna pravila.

OPOMBE:

- Če se pojavijo napake v zvezi z Windows varnostna prijava, ko ste se poskušali prijaviti, onemogočite in znova omogočite možnost Dell varnostna prijava.
- Če želite podrobnejše informacije o določenem sporočilu o napaki, pojdite na wave.com/support/Dell.

Ponovni zagon sistema

Ponovni zagon sistema je funkcija, ki se uporablja za odstranjevanje vseh uporabniških podatkov iz vse varnostne strojne opreme na platformi, to se uporablja, na primer za spremembo uporabe računalnika. Ta možnost bo zbrisala vsa gesla v sistemu, razen Windows uporabniška gesla, kot tudi vse podatke v strojni opremi (npr. ControlVault, TPM in čitalcev prstnih odtisov). Za samo-širfirne pogone, ta funkcija tudi onemogoči varovanje podatkov, tako je možen dostop do podatkov pogona.

Potrditi morate, da se zavedate ponastavitve sistema in nato kliknite **Naprej**. Če želite ponastaviti sistem, boste morali vnesti geslo za vsako varnostno napravo, če so bile nastavljene:

- TPM lastnik
- ControlVault skrbnik
- BIOS skrbnik
- BIOS sistem (pre-Windows)
- Trdi disk (BIOS)
- Self-Encrypting Drive skrbnik

OPOMBA: Za samo-šifrirne pogone, je potrebno geslo skrbnika pogona; ne vsa gesla pogonov uporabnikov.

Pomembno! Edini način, da obnovite vse zbrisane podatke, ko ponastavite sistem, je obnovitev iz prej shranjenih arhivov. Če nimate arhivov, so ti podatki neobnovljivi. Za samo-šifrirne pogone, se zbrišejo samo podatki namestitve, osebni podatki na disku niso zbrisani.

Credential Archive & Obnovitev

Credential Archive and Restore funkcionalnost se uporablja za varnostno kopiranje in obnovitev vseh uporabniških poverilnic (prijavo in šifrirne podatke), shranjene v ControlVault in Trusted Platform Module (TPM). Varnostno shranjevanje teh podatkov je pomembno, za ponovno obnovitev računalnika ali za obnovo podatkov v primeru okvare strojne opreme. V tem primeru lahko enostavno, iz shranjene arhivirane datoteke, obnovite vse vaše poverilnice na nov računalnik.

Lahko se odločite za arhiviranje ali obnovitev poverilnic za posameznega uporabnika ali pa za vse uporabnike sistema.

Poverilnice uporabnika so sestavljene iz podatkov, ki se uporabljajo v pre-Windows-u, kot so vnešeni podatki prstnih odtisov in pametnih kartic in ključi shranjeni v TPM. TPM bo ustvaril ključe, kot jih zahtevajo aplikacije za varnost, na primer, ustvarjanje digitalnega potrdila bo ustvarilo ključe v TPM.

OPOMBA: Če želite ugotoviti ali je TPM ključe mogoče arhivirati z **Dell Data Protection | Access**, si oglejte dokumentacijo za varno uporabo. Na splošno, so aplikacije z uporabo “Wave TCG-Enabled CSP” podprte za ustvarjanje ključev.

Archiving Credentials
Za arhiviranje poverilnic morate storiti naslednje:

- Navedite, ali arhivirate poverilnice za sebe ali za vse uporabnike na sistemu.
- Omogočite preverjanje pristnosti za varno strojno opremo z vnosom sistemskega (pre-Windows) gesla, gesla ControlVault skrbnika in geslo TPM lastnika.
- Ustvarite geslo poverilnice za varnostno kopiranje podatkov.
- Navedite podatke o lokaciji arhiva z uporabo gumba **Poišči**. Podatki arhiva morajo biti na izmenljivem mediju, kot je pomnilniški ključek USB ali omrežni pogon, da bi se tako zaščitili pred odpovedjo trdega diska.

Pomembne opombe:
- Zabeležite podatke o lokaciji arhiva, ker bo uporabnik te informacije potreboval za obnovo informacij o poverilnicah.
- Zabeležite podatke o geslu varnostne kopije, da zagotovite ponovno nalaganje podatkov. To je pomembno, saj tega gesla ni mogoče obnoviti.
- Če ne poznate TPM gesla lastnika, se obrnite na skrbnika sistema ali poglejte v računalniška navodila za nalaganje TPM.

Restoring Credentials
Za obnavljanje poverilnic morate storiti naslednje:

- Navedite, ali obnavljate poverilnice za sebe ali za vse uporabnike na sistemu.
- Poiščite podatke o lokaciji arhiva in izberite arhivske datoteke.
- Vnesite geslo za poveritev obnovitve, ki je bila ustvarjena, ko ste naredili arhiv.
- Omogočite preverjanje pristnosti za varnostno strojno opremo z vnosom sistemskega (pred-Windows) gesla, gesla ControlVault skrbnika in geslo TPM lastnika.

OPOMBE:
- Če se pojavi napaka, ki navaja, da obnovitev poverilnic ni uspela in ste večkrat poskušali opraviti obnovitev, poskusite obnoviti drugo datoteko arhiva. Če to ni uspešno, ustvarite nov arhiv poverilnic in poskusite obnoviti iz novega arhiva.

- Če se pojavi napaka, ki navaja, da TPM ključev ni bilo mogoče obnoviti, ustvarite arhiv poverilnic, nato pa zbrišite TPM v samem BIOS-u. Za brisanje TPM-a, ponovno zaženite računalnik, pritisnite tipko **F2** ob zaganjanju, da vstopite v BIOS nastavitve, nato pa se premanite v Security>TPM Security. Nato ponovno vzpostavite TPM lastništvo in poskusite znova obnoviti poverilnice.
- Če želite podrobnejše informacije o določenem sporočilu o napaki, pojdite na wave.com/support/Dell.

Upravljanje z gesli

V oknu Upravljanje z gesli, lahko skrbnik ustvari ali spremeniti vsa varnostna gesla na vašem sistemu:

- Sistem (znan tudi kot Pre-Windows) *
- Skrbnik*
- Trdi disk*
- ControlVault
- TPM lastnik
- TPM Master
- TPM Password Vault
- Self-Encrypting Drive

OPOMBE:

- Samo tista gesla bodo prikazana, ki veljajo za trenutno konfiguracijo platforme; tako da se bo to okno spremenilo, ki temelji na konfiguracijo in statusu sistema.
- Tista zgornja gesla z * poleg njih so BIOS gesla in se lahko spremenijo tudi preko sistema BIOS.
- BIOS gesel ni mogoče ustvariti ali spremeniti, če je skrbnik za BIOS onemogočil spremembe gesla.
- S klikom na povezavo **namestitev**samo-šifrirnega pogona zažene Self-Drive Encrypting namestitveni čarovnik, ko kliknete **upravljanje** to omogoča uporabniku, da spremeni en ali več Self-Encrypting Drive gesel.
- S klikom na povezavo **upravljanje** za TPM Password Vault prikaže okno, v katerem si lahko ogledate ali spremenite gesla, da zaščitite vaše TPM ključe. Ko je ustvarjen TPM ključ, ki zahteva geslo, je geslo naključno ustvarjeno in vstavljeno v trezor. Ne morete upravljati TPM Password Vault, dokler ne ustvarite TPM Master geslo.

Windows GesloPravila zapletenosti

Dell Data Protection | Access zagotavlja, da bo naslednje geslo v skladu z Windows pravili zapletenosti gesel za naprave:

- TPM Geslo lastnika

Če želite za napravo določiti pravila zapletenosti gesel za Windows, sledite naslednjim korakom:

1. Vstopite v nadzorno ploščo.
2. Dvokliknite Skrbniška orodja.
3. Dvokliknite Lokalna varnostna politika.
4. Razširite pravila računa in izberite Pravila gesel.

Naprave

Okno Naprave uporabljajo skrbniki za upravljanje vseh varnostnih naprav, ki so nameščene na njihovem sistemu. Za vsako napravo si lahko ogledate stanje in dodatne podrobne podatke, kot je različica firmware. Kliknite **prikaz**, da si ogledate podatke za vsako napravo ali **skrij** za zapiranje tega področja. Naprave za upravljanje so naslednje, v odvisnosti od vsebnosti na vaši platformi:

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

Trusted Platform Module (TPM)

TPM varnostni čip je treba omogočiti in določiti lastništvo TPM, da se uporabijo napredne varnostne funkcije, ki so na voljo z **Dell Data Protection | Access** in samim TPM.

Okno Trusted Platform Module v področju **Upravljanje naprav** se prikaže le tedaj, ko je TPM zaznan na vašem sistemu.

TPM upravljanje

Te funkcije omogočajo skrbniku sistema TPM upravljanje.

Stanje

Za TPM prikaže status *aktiven* ali *neaktiven*. Status "Aktiven" pomeni, da je bil TPM omogočen v BIOS-u in je pripravljen za namestitev (tj. lahko se sprejme lastništvo) TPM se ne more upravljati in do njegove varnostne funkcije ni mogoče dostopati, če TPM ni aktiven (omogočen).

Če je TPM odkrit na sistemu, vendar pa ni aktiven (omogočen), ga lahko omogočite s klikom na povezavo **aktiviraj** v tem oknu, brez vstopa v sistem BIOS. Po tem, ko je omogočen, je potrebno za uporabo TPM te funkcije računalnik znova zagnati. Med ponovnim zagonom, se bodo v nekaterih primerih prikazala obvestila s prošnjo, da sprejmete spremembe.

OPOMBA: Možnost, da bi omogočili (aktivirali) TPM iz te aplikacije, po vsej verjetnosti ni podprta na vseh platformah. Če ni podprta, ga morate omogočiti v sistemskem BIOS-u. Če želite to narediti, ponovno zaženite vaš sistem, pritisnite tipko **F2** za vstop v BIOS nastavitve, preden se Windows naloži, potem pa poiščite Security>TPM Security in vključite TPM

Lahko tudi *deaktivirate* TPM od tukaj s klikom na povezavo **deaktiviraj**; z izklopom TPM ne bodo več na voljo napredne varnostne funkcije. Izklop pa ne spremeni katero koli od TPM nastavitev ali izbriše ali spremeni informacije ali ključe, ki so shranjeni v TPM.

Lastništvo

Prikaže status lastništva (tj. "v lasti") in vam omogoča, da vzpostavite ali spremenite TPM lastnika. TPM lastništvo se mora vzpostaviti za razpolaganje z varnostnmi značilnostmi. Preden se lahko oblikuje lastništvo, mora biti TPM omogočen (aktiviran).

Postopek za določitev lastništva je sestavljen iz uporabnikovega (s pravicami skrbnika) ustvarjanja TPM gesla lastnika. Ko je opredeljeno geslo, je lastništvo oblikovano in TPM je pripravljen za uporabo.

OPOMBA: TPM Geslo lastnika mora biti skladno z vašim sistemom, glede na Windows zapletenost pravil za gesla.

Pomembno! Pomembno je, da ne boste izgubili ali pozabili TPM geslo lastnika, saj je zahtevano za dostop do naprednih funkcij varnosti TPM v **Dell Data Protection | Access**.

Zaklenjeno

Prikaže status za TPM *zaklenjeno* ali *nezaklenjeno*. "Zaklepanje" je TPM varnostna funkcija; TPM bo prešel v zaklenjeno stanje, ko bo vnešeno določeno število napačnih vnosov TPM gesel lastnika. TPM lastnik lahko od tukaj odklene TPM ; zahtevan pa je vnos TPM gesla lastnika.

OPOMBE:

- Če se pojavi napaka, ki navaja, da ni bilo mogoče oblikovati lastništva TPM, zbrišite TPM v sistemskem BIOS-u in poskusite ponovno vzpostaviti lastništvo. Za brisanje TPM, ponovno zaženite računalnik, pritisnite tipko **F2** ob zaganjanju, da vstopite v BIOS nastavitve, nato pa se premaknite v Security>TPM Security.

- Če se pojavi napaka, ki navaja, da TPM gesla lastnika ni bilo mogoče spremeniti, arhivirajte TPM podatke (poverilen arhiv), zbrišite TPM v BIOS-u, ponovno vzpostavite lastništvo za TPM in obnovite TPM podatke (obnovitev poverilnic).
- Če želite podrobnejše informacije o določenem sporočilu o napaki, pojdite na wave.com/support/Dell.

Dell ControlVault®

Dell ControlVault® (CV) je varno shranjevanje v strojni opremi za uporabniške poverilnice, ki se uporabljajo med prijavo v pre-Windows (npr. gesla uporabnika ali vpisani podatki o prstnih odtisih). Okno ControlVault v **Upravljanje naprav** se prikaže le, če je ControlVault zaznan na vašem sistemu.

ControlVault Management

Te funkcije omogočajo skrbniku sistema upravljanje za sistemski ControlVault.

Stanje
Prikaže ControlVault status *aktiven* ali *neaktiven*. Status "Neaktiven" pomeni, da ControlVault ni na voljo za shranjevanje na vaš sistem. Poglejte Dell sistemsko dokumentacijo, da ugotovite, če sistem vsebuje ControlVault.

Geslo
Označuje, če je bilo ControlVault geslo skrbnika nastavljeno in vam omogoča, da nastavite geslo ali pa ga spremenite (če je eno geslo že nastavljeno). Samo skrbniki sistema lahko nastavijo ali spremenijo geslo. ControlVault skrbniško geslo je treba nastaviti, da bi lahko naredili naslednje:

- Izvedite arhiv ali obnovitev poverilnic.
- Pobrišite uporabniške podatke (za vse uporabnike).

OPOMBA: Če izvajate poskus arhiviranja ali obnovitve, ko ControlVault skrbniško geslo ni bil določeno, ste pozvani, da ustvarite novega (če ste skrbnik).

Vnešeni uporabniki
Prikazuje, ali ima kateri od uporabnikov vpisane poverilnice za prijavo (npr. gesla, prstne odtise ali pametne kartice, podatke), ki so trenutno shranjeni v ControlVault.

Brisanje podatkov uporabnika
Podatke v ControlVault mogoče do neke točke ni treba zbrisati, na primer, če imajo uporabniki težave z uporabo ali s vpisom poverilnic v pre-Windows za preverjanje pristnosti. Vsi podatki shranjeni v ControlVault so lahko iz tega okna zbrisani za posameznega uporabnika ali za vse uporabnike.

The ControlVault skrbniško geslo je treba vnesti za izbris vseh uporabniških podatkov na platformi. Če bodo poverilnice v pre-Windows vnešene, boste opomnjeni za vpis sistemskega gesla za pre-Windows. Ko zbrišete vse uporabniške podatke, sta ControlVault skrbniško geslo in sistemsko geslo ponastavljena; upoštevajte, da je to edini način, da zbrišete ControlVault skrbniško geslo.

OPOMBA: Ko boste zbrisali vse uporabniške podatke, morate ponovno zagnati računalnik. Pomembno je, da ponovno zaženete zaradi pravilnega delovanja vašega sistema.

ControlVault skrbniškega gesla ni treba nastaviti, da bi zbrisali poverilnico enega samega uporabnika. Ko kliknete **zbriši podatke uporabnika**, ste pozvani, da izberete uporabnika, za katerega želite zbrisati ControlVault poverilnice. Ko izberete uporabnika, morate podati sistemsko geslo (samo, če so vnešene pre-Windows poverilnice).

OPOMBE:

- Če se pojavi napaka, ki navaja, da ControlVault skrbniškega gesla ni mogoče ustvariti, morate arhivirati vaše poverilnice, zbrisati vse uporabniške podatke iz ControlVault, ponovno zagnati računalnik in poskusiti ustvariti geslo.

- Če se pojavi napaka, ki navaja, da poverilnic ni mogoče izbrisat iz ControlVault za enega uporabnika, morate arhivirati vaše poverilnice, poskusiti zbrisati vse uporabniške podatke, nato pa ponovno poskusiti zbrisati podatke za posameznega uporabnika.
- Če se pojavi napaka, ki navaja, da poverilnic ni mogoče izbrisati iz ControlVault za vse uporabnike, morate predvideti opraviti ponovni zagon sistema. **Pomembno!** Preglejte teme pomoči za Ponovni zagon sistema preden izvedete ponovni zagon, saj bo to zbrisalo VSE varnostne podatke uporabnika.
- Če se pojavi napaka, ki navaja, da podatke ControlVault in TPM ni bilo mogoče varnostno shraniti, onemogočite TPM v sistemskemBIOS-u. To naredite tako, da ob ponovnem zagonu računalnika, pritisnete tipko **F2**, ko se začne zagon, da dostopate do BIOS nastavitev, nato pa poiščete Security>TPM Security. Nato znova omogočite TPM in poskusite znova arhivirati vaše ControlVault podatke.
- Če želite podrobnejše informacije o določenem sporočilu o napaki, pojdite na wave.com/support/Dell.

Self-Encrypting Drives: Napredno

Dell Data Protection | Access upravlja na osnovi strojne opreme z varnostnimi funkcijami samo-šifrirnih pogonov, ki imajo šifriranje podatkov vključeno v pogon strojne opreme. To upravljanje se uporablja za zagotavljanje, da lahko imajo dostop le pooblaščeni uporabniki šifrirnih podatkov, ko je omogočeno zaklepanje pogona.

Okno Self-Encrypting Drive v **Upravljanje naprav** se prikaže le, ko je prisotenih na vašem sistemu eden ali več samo-šifrirnih pogonov (SED).

Pomembno! Ko je pogon nastavljen, je omogočeno self-encrypting drive varovanje podatkov in zaklepanje pogona.

Upravljanje pogona

Te funkcije omogočajo skrbniku pogona upravljanje varnostnih nastavitev. Spremembe varnostnih nastavitev pogona začnejo veljati potem, ko je bil disk izključen iz napajanja.

Zaščita podatkov

Prikaže status *omogočeno* ali *onemogočeno* za varstvo podatkov samo-šifrirnih pogonov. Status "omogočeno" pomeni, da je bila nastavljena varnost diska, vendar dokler je *zaklepanje* pogona vklopljeno, uporabniki za dostop na pogon ne bodo mogli overjati v pre-Windows.

Od tod lahko onemogočite zaščito podatkov samo-šifrirnih pogonov. Ko je onemogočen, so vse napredne varnostne funkcije samo-šifrirnega pogona izklopljene in pogon deluje kot standardni pogon. Onemogočanje varovanja podatkov prav tako izbriše vse varnostne nastavitve, vključno s poverilnicami skrbnika in uporabnikov pogona. Ta funkcija pa ne spremeni ali odpravi vseh uporabniških podatkov na disku.

Zaklepanje

Prikaže status *omogočeno* ali*onemogočeno* za samo-šifrirne pogone. Poglejte temo Self-Encrypting Drive o informacijah, kako se obnaša zaklenjen pogon.

Morda bo potrebno začasno onemogočiti zaklepanje pogona, kar lahko storite od tukaj. To ni priporočljivo, saj niso potrebne poverilnice za dostop do pogona, ko je zaklepanje pogona onemogočeno, tako da lahko ima vsak uporabnik platforme dostop do podatkov pogona. Onemogočanje zaklepanja pogonov neizbriše varnostnih nastavitev, vključno s poverilnicami skrbnika pogonov in uporabnikov pogona, ali vseh drugih uporabniških podatkov na disku.

POZOR! Če odstranite aplikacijo **Dell Data Protection | Access**, morate najprej onemogočiti self-encrypting drive zaščito podatkov in odklepanje pogona.

Skrbnik pogona

Prikaže trenutnega skrbnika pogona. Skrbnik pogona lahko spremeni, kateri uporabnik je lahko od sedaj naprej skrbnik. Novi skrbnik mora biti veljaven Windows uporabnik na sistemu s skrbniškimi pravicami. Na sistemu je lahko samo en skrbnik pogona.

Uporabniki pogona

Prikaže vnešene uporabnike pogona in število trenutno vpisanih uporabnikov. Največje število uporabnikov, ki je podprtih, temelji na samo-šifrirnem pogonu (trenutno 4 uporabnike za pogone Seagate in 24 za pogone Samsung).

Windows gesloSync
Windows password synchronization (WPS) funkcija samodejno nastavi gesla uporabnikov Self-Encrypting Drive, da je enako kot njihovo geslo za Windows. Ta funkcija se ne izvaja za skrbnika pogona, ampak se uporablja samo za uporabnike pogona. Funkcionalnost WPS se lahko uporablja v okoljih podjetij, v katerih se morajo gesla spremenjati v določenih časovnih intervalih (npr. vsakih 90 dni); s to možnostjo omogočeno, se gesla vsem uporabnikom samo-šifrirnega pogona samodejno posodobijo, ko se spremenijo ta Windows gesla.

OPOMBA: Ko je omogočena sinhronizacija Windows gesel (WPS), se uporabnikovo geslo Self-Encrypting Drive ne more spreminjati; njihovo geslo za Windows je treba spremeniti, da bi se samodejno posodabljalo geslo pogona.

Zapomni zadnjouporabniško ime
Ko je ta možnost omogočena, se zadnje vpisano uporabniško ime privzeto prikaže v polju **Uporabniško ime**zaslona pre-Windows overjanja.

Uporabniško imelzbira
Ko je ta možnost omogočena, lahko uporabniki vidijo vse pogone v polju **Uporabniško ime**zaslona pre-Windows overjanja.

Kriptografskilzbris
Ta možnost se lahko uporablja za "izbris" vseh podatkov samo-šifrirnega pogona To dejansko ne zbriše podatkov ampak ključe, ki se uporabljajo za šifriranje podatkov, s čimer postanejo podatki neuporabni. Ni načina, da se podatki pogona po kriptografskem zbrisu obnovijo; tudi zaščita podatkov samo-šifrirnega pogona je onemogočena in pogon je pripravljen za spremembo namembnosti.

OPOMBE:
- Če dobite napake v zvezi s self-encrypting drive funkcijo upravljanja, popolnoma ugasnite računalnik (ne ponovnega zagona) in ga znova zaženite.
- Če želite podrobnejše informacije določenega sporočila o napaki, pojdite na wave.com/support/Dell.

Authentication Device Information

Okno informacije Authentication Device v **Device Management** prikazuje informacije in status za vse povezane naprave na sistemu za preverjanje pristnosti (tj. čitalec prstnih odtisov, običajne ali brezkontaktne čitalnike pametne kartice).

Tehnična pomoč

Tehnično pomoč za program **Dell Data Protection | Access** lahko najdete na http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP

The Wave Systems Trusted Computing Group (TCG)-enabled Cryptographic Service Provider (CSP) je vključen z **Dell Data Protection | Access** aplikacijo in je na voljo za uporabo, kadar je potreben CSP - bodisi neposredno iz aplikacije ali z izbiro s seznama nameščenih CSP-jev. Če je mogoče, izberite "Wave TCG-Enabled CSP" za zagotovitev, da si TPM ustvarja ključe in da so ti ključi in gesla upravljani z **Dell Data Protection | Access**.

The Wave Systems TCG-enabled CSP omogoča aplikacijam uporabo funkcij, ki so na voljo na TCG skladnih platformah neposredno preko MSCAPI. To je TCG-enhanced MSCAPI CSP modul, ki omogoča asimetrično funkcionalnost ključev na TPM in povečuje izboljšano varnost, ki jo omogoča TPM, neodvisno od posebnih zahtev prodajalca, glede dobavitelja Trusted Software Stack (TSS).

OPOMBA: Če TPM ključi, ki jih ustvari Wave TCG-enabled CSP zahtevajo geslo in je uporabnik ustvaril TPM Master geslo, bodo posamezna ključna gesla naključno ustvarjena in shranjena v TPM Password Vault.