Dell zaštita podataka | Početak pristupa

Dell Data Protection | Access Glavna stranica je početna točka za pristup značajkama ove aplikacije. Iz ovog prozora, možete pristupiti sljedećem:

Čarobnjak za pristup sustavu
Mogućnosti pristupa
Samokodirajući pogon
Napredne mogućnosti

U donjem desnom kutu prozora se nalazi poveznica pod nazivom **napredno** na koju možete kliknuti da biste pristupili naprednim mogućnostima.

Iz naprednih mogućnosti možete kliknuti na poveznicu **vrh** u u donjem desnom kutu prozora da biste se vratili na glavnu stranicu.

Čarobnjak za pristup sustavu

Čarobnjak za pristup sustavu se pokreće automatski kad se prvi put pokrene aplikacija **Dell Data Protection | Access**. Čarobnjak će vas voditi kroz podešavanje svih aspekata sigurnosti na vašem sustavu, uključujući kako (npr. samo zaporka ili otisak prsta i zaporka) i kada (kod ulaska u sustav Windows, prije, ili oboje) se želite prijaviti u sustav. Osim toga, ako vaš sustav ima samokodirajući pogon, možete ga podesiti preko ovog čarobnjaka.

Administratorske funkcije

Korisnici koji su postavljeni s administratorskim ovlastima na sustavu Windows imaju pravo obavljati sljedeće funkcije u aplikaciji **Dell Data Access | Protection**, što standardni korisnici ne mogu:

- Postavi / promijeni zaporku sustava (prije Windowsa)
- Postavi / promijeni zaporku tvrdog diska
- Postavi / promijeni zaporku administratora
- Postavi / promijeni TPM zaporku vlasnika
- Postavi / promijeni zaporku ControlVault administratora
- Ponovno pokreni sustav
- Arhiviraj i vrati akreditacije
- Postavi / promijeni PIN administratora pametne kartice
- Obriši / ponovno pokreni pametnu karticu
- Uključi / isključi Dell Secure Login (sigurnu prijavu) na sustav Windows
- Postavi smjernice prijave na sustav Windows
- Upravljaj samokodirajućim pogonima, uključujući:
    - Uključi / isključi zaključavanje samokodirajućeg pogona
    - Uključi / isključi sinkrinizaciju Windows zaporki (WPS)
    - Uključi / isključi jednokratnu prijavu (SSO)
    - Izvrši kriptografsko brisanje

Udaljeno upravljanje

Vaša organizacija može postaviti okolinu u kojoj se sigurnosne funkcijama aplikacije **Dell Data Protection | Access** na višestrukim plaformama upravlja centralno (tj. udaljeno upravljanje). U tom se slučaju sigurnosna infrastruktura sustava Windows, kao što je Aktivni direktorij, može koristiti za sigurnosno upravljanje specifičnim značajkama pomoću aplikacije **Dell Data Protection | Access**.

Kad se računalom upravlja daljinski (tj. kad je “u vlasništvu” udaljenog administratora), lokalna administracija funkcijom **Dell Data Protection | Access** se može isključiti; prozoru upravljanja aplikacijom se ne može pristupiti lokalno. Upravljanje sljedećim funkcijama se može izvršiti udaljeno:

- Trusted Platform Module (TPM)
- ControlVault
- Pretprijava u sustav Windows
- Ponovno pokreni sustav
- BIOS zaporke
- Smjernice prijave u sustav Windows
- Samokodirajući pogoni
- Prijava otiskom prsta i pametnom karticom

Da biste zatražili više informacija o uporabi Wave Systems' EMBASSY® Remote Administration Servera (ERAS) za daljinsko upravljanje, molimo kontaktirajte svog Dell prodavaća ili idite na dell.com.

Mogućnosti pristupa

Iz prozora Mogućnosti pristupa, možete podesiti kako možete dobiti pristup vašem sustavu.

Ako imate bilo kakve podešene opcije **Dell Data Protection | Access**, one će biti prikazane na glavnoj stranici s dostupnim mogućnostima (npr., promijeni zaporku za pretprijavu na sustav Windows). Te dostupne opcije su prečaci koji vas, kad se klikne na njih, vode na odgovarajući prozor za obavljanje određene zadaće (npr. promjena zaporke prije sustava Windows ili prijava drugog otiska prsta).

Opće
Prvo, možete odrediti kad se prijaviti (Windows, prije sustava Windows ili oboje) i kako (npr. otisak prsta i zaporka). Možete odabrati jednu ili dvije opcije kako se prijaviti; one uključuju kombinacije otiska prsta, pametne kartice i zaporke. Navedene mogućnosti su zasnovane na smjernicama o prijavi koje se primjenjuju u vašem okružju i što je podržano na platformi.

otisak prsta
Ako vaš sustav sadrži čitač otisaka prstiju, možete prijaviti ili ažurirati otiske prstiju za uporabu kod prijave na sustav. Kad jednom prijavite otiske prsta, možete provući prijavljene prste na čitaču otisaka prstiju na vašem sustavi za pristup vašem sustavu kod Windowsa, prije sustava Windows ili oboje (ovisno o tome što ste naznačili u Općim mogućnostima pristupa). Za više informacija, pogledajte Prijava otiska prsta.

Pretprijava u sustav Windows
Ako ste odredili da se korisnici moraju prijaviti prije sustava Windows, morate podesiti zaporku sustava (nekad se zove zaporka prije sustava Windows) za pristup prije sustava Windows. Kad je jednom to podešeno, administrator može bilo kada promijeniti zaporku.

Iz ovog prozora možete također isključiti pretprijavu u sustav Windows; morat ćete unijeti vašu trenutnu zaporku sustava, provjeriti da je zaporka točna, zatim kliknuti na tipku **Isključi**.

Pametna kartica
Ako ste odredili da korisnici za prijavu moraju koristiti pametnu karticu, morate prijaviti jednu ili više tradicionalnih (kontaktnih) ili bezkontaktnih pametnih kartica. Kliknite na vezu **Prijavi dodatnu pametnu karticu** da biste pokrenuli čarobnjak okružja pametne kartice. Prijava znači podešavanje vaše pametne kartice za uporabu kod prijave.

Kad prijavite pametnu karticu, možete promijeniti ili podesiti PIN za tu karticu pomoću veze **Promijeni ili podesi PIN moje pametne kartice**.

Pretprijava u sustav Windows

Kad se odabere pretprijava u sustav Windows, morate izvršiti provjeru (zaporkom, otiskom prsta ili pametnom karticom) kad se sustav uključi, prije učitanja sustava Windows. Funkcija pretprijave u sustav Windows daje dodatnu sigurnost sustavu, držeći neovlaštene korisnike podalje od kompromitiranja sustava Windows i pristupa računalu (npr. kad je ukradeno).

Iz prozora pretprijave na sustav Windows, administratori mogu postaviti pretprijavu u sustav Windows login, ili stvoriti ili promijeniti zaporku za pretprijavu u Windows (sustav); ako je ova zaporka već postavljena, možete isključiti pretprijavu na sustav Windows iz ovog prozora. Postavljanje pretprijave na sustav Windows će pokrenuti čarobnjaka koji će uraditi sljedeće:

- Zaporka sustava: postaviti zaporku sustava (također poznata kao zaporka prije sustava Windows) za pristup prije sustava Windows. Ova se zaporka također koristi kao pričuvna u slučaju u kojima korisnik ima dodatne čimbenike provjere (npr. za dobivanje pristupa sustavu ako ima problema s čitačem otiska prsta).
- Otisak prsta ili pametna kartica: Postavite otisak prsta ili pametnu karticu za uporabu kod prijave na sustav Windows, i odredite da li će se ovaj čimbenik provjere koristiti umjesto,ili uz zaporke prije sustava Windows.
- Jednostruka prijava: Kao zadano, vaša provjera prije sustava Windows (zaporka, otisak prsta ili pametna kartica) će se koristiti da vas automatski prijavi i u sustav Windows (ovo se zove "Jednostruka prijava"). Da biste isključili ovu zaporku, odaberite potvrdnu kućicu "Želim se ponovno prijaviti u sustav Windows".
- Ako je BIOS zaporka tvrdog diska postavljena osim zaporke prije sustava Windows, također ćete imati mogućnost promijeniti ili isključiti zaporku tvrdog diska.

NAPOMENA: Nije svim čitačima otisaka prstiju omogućena uporaba prijave prije sustava Windows. Ako vaš čitač nije kompatibilan, moći ćete prijaviti otiske prsta samo za prijavu na sustav Windows. Da biste otkrili da li je određeni čitač otisaka prstiju kompatibilan, javite se vašem administratoru sustava ili idite na support.dell.com da biste dobili popis podržanig čitača otisaka prstiju.

Isključi pretprijavu u sustav Windows
Iz ovog prozora možete također isključiti pretprijavu u sustav Windows; morat ćete unijeti vašu trenutnu zaporku za pretprijavu na windows (sustav), provjeriti da je zaporka točna, zatim kliknuti na tipku **Isključi**. Imajte na umu da kad isključite pretprijavu na sustav Windows, svi prijavljeni otisci prstiju ili pametne kartice ostaju prijavljeni.

Prijava / uklanjanje otisaka prstiju

Korisnici mogu registrirati ili ažurirati otiske prsta koji se mogu koristiti za provjeru sustava za pretprijavu ili prijavu na sustav Windows. Na pločici Otisci prsta, slike ruku će prikazati koji su prsti korišteni, ako jesu. Klikom na vezu **Prijavi drugi** se pokreće čarobnjak za prijavu otiska prsta, koji vas vodi kroz postupak prijave. "Prijava" znači spremanje otiska prsta za uporabu kod prijave. Morate imati pravilno instalirani i podešeni valjani čitač otisaka prsta da bi se prijavljivali otisci prsta.

NAPOMENA: Ne mogu se svi čitači prsta koristiti za prijavu prije sustava Windows. Ako se pokušate prijaviti za prijavu prije sustava Windows s nekompatibilnim čitačem, prikazat će se poruka o pogrešci. Da biste otkrili da li je određeni čitač otisaka prstiju kompatibilan, javite se vašem administratoru sustava ili idite na support.dell.com da biste dobili popis podržanig čitača otisaka prstiju.

Kod prijave otisaka prsta, od vas će se tražiti da unesete zaporku za sustav Windows da biste potvrdili svoj identitet. Ako je to potrebno prema smjernicama, od vas će se zatražiti da unesete i svoju zaporku prije sustava Windows (zaporku sustava) . Zaporka prije sustava Windows se može koristiti da biste dobili pristup sustavu ukoliko ima problema s čitačem otiska prsta.

NAPOMENE:

- Preporučuje se da prijavite najmanje dva otiska prsta tijekom postupka prijave.
- Morate paziti da su otisci prsta pravilno prijavljeni prije uključivanja mogućnosti prepoznavanja otiska prsta.
- Ako promijenite čitače otisaka prsta na sustavu, morate ponovno prijaviti prste s novim čitačem. Stalno prebacivanje između dva različita čitača otisaka prsta se ne preporučuje.
- Ako vidite stalno poruke "senzor je izgubio fokus" kad prijavljujete otiske prstiju, to može značiti da računalo ne prepoznaje čitač otisaka prsta. Ako je čitač otisaka prstiju vanjski, isključite i ponovno uključite čitač otisaka prsta jer to često rješava problem.

Brisanje prijavljenih otisaka prsta
Možete ukloniti prijavljene otiske prsta klikom na vezu **Ukloni otisak prsta** ili klikom na (da biste maknuli odabir) prijavljeni prst u čarobnjaku za prijavu otisaka prsta.

Da biste uklonili specifičnog korisnika koji je prijavio otiske prsta za provjeru prije sustava Windows, administrator može maknuti oznaku sa svih otisaka prsta prijavljenog za tog korisnika.

NAPOMENA: Ako dobijete bilo kakve pogreške tijekom postupka prijave otisaka prsta, možete pogledati wave.com/support/Dell za dodatne informacije.

Prijava pomoću pametnih kartica

Dell Data Protection | Access vam daje mogućnost uprabe tradicionalne (kontaktne) ili bezkontaktne pametne kartice za prijavu na vaš Windows račun ili provjeru prije sustava Windows. Klikom na vezu **Prijavi drugu pametnu karticu** se pokreće čarobnjak za prijavu pametne kartice, koji vas vodi kroz postupak prijave. "Prijava" znači podešavanje vaše pametne kartice za uporabu kod prijave.

Morate imati pravilno instalirani i podešeni valjani uređaj za provjeru pametnih kartica da bi ste izvršili prijavu.

NAPOMENA: Da biste otkrili da li je određeni uređaj kompatibilan, javite se vašem administratoru sustava ili idite na support.dell.com da biste dobili popis podržanih pametnih kartica.

Prijava
Kod prijave pametne kartice, od vas će se tražiti da unesete zaporku za sustav Windows da biste potvrdili svoj identitet. Ako je to potrebno prema smjernicama, od vas će se zatražiti da unesete i svoju zaporku prije sustava Windows (zaporku sustava) . Zaporka prije sustava Windows se može koristiti da biste dobili pristup sustavu ukoliko ima problema s čitačem pametne kartice.

Tijekom prijave, od vas će se zatražiti PIN pametne kartice, ako je postavljen. Ako vaše smjernice zahtijevaju PIN a on nije postavljen, od vas će se zatražiti da ga stvorite.

NAPOMENE:

- Kad se korisnik prijavi za pametnu karticu za uporabu prije sustava Windows, on/ona se ne mogu ukloniti.
- Standardni korisnici mogu promijeniti korisnički PIN na pametnoj kartici, a administrator može promijeniti i administratorski PIN i korisnički PIN.
- Administrator također može ponovno pokrenuti pametnu karticu; kad se jednom ponovno pokrene, pametna kartica se ne može koristiti za prijavu na sustav Windows ili prije sustava Windows dok se ponovno ne prijavi.

NAPOMENA: Za provjeru TPM certifikata, administratori mogu prijaviti TPM certifikate preko postupka prijave pametne kartice za Microsoftov sustav Windows. Administratori moraju odabrati "Wave TCG-Enabled CSP" kao davatelja kruptografskih usluga umjesto Smartcard CSP za kompatibilnost s ovom aplikacijom. Osim toga, Dell Secure login mora biti uključen s odgovarajućim smjernicama vrste provjere za klijenta.

NAPOMENA: Ako dobijete pogrešku koja kaže da usluga pametne kartice ne radi, možete uključiti / ponovno pokrenuti ovu uslugu na sljedeći način:

- Idite do prozora s administrativnim alatima s upravljačke ploče, odaberite Uslugu, zatim desnom tipkom kliknite na Pametnu karticu i odaberite Pokreni ili ponovno pokreni.
- Ako želite detaljnije informacije o određenoj poruci pogreške, idite na wave.com/support/Dell.

Samokodirajući pogon

Dell Data Protection | Access upravlja hardverski zasnovanim sigurnosnim funkcijama samokodirajućih pogona, koji imaju kodiranje podataka uključene u hardver pogona. Ova funkcija se koristi da bi se osiguralo da samo ovlašteni korisnici mogu pristupiti kodiranim podacima (kad je uključeno zaključavanje pogona).

Prozoru samokodirajućeg pogona se pristupa klikom na donju pločicu **Samokodirajući pogon**. Ova se pločica prikazuje samo kad je prisutan jedan ili više samokodirajućih pogona (SEDs) na vašem sustavu.

Kliknite na vezu **Instalacija** da biste pokrenuli čarobnjak instalacije samokodirajućeg pogona. U ovom ćete čarobnjaku stvoriti zaporku administratora pogona, napraviti sigurnosnu kopiju zaporke i primijeniti postavke kodiranja pogona. Samo administratori sustava mogu pristupiti čarobnjaku instalacije samokodirajućeg pogona.

Važno! Kad je pogon postavljen, zaštita podataka samokodirajućeg pogona i zaključavanje pogona su "uključeni". Kad se pogon zaključan, primjenjuje se sljedeće ponašanje:

- Pogon ulazi u *zaključan* način rada kad god se isključi napajanje pogona.
- Pogon se neće podignuti ako korisnik ne unese točno korisničko ime i zaporku (ili otisak prsta) na zaslonu prijave prije sustava Windows. Prije nego je uključeno zaključavanje pogona, podacima na pogonu može pristupiti bilo koji korisnik na računalu.
- Pogon je osiguran čak i ako se uključi u drugo računalo kao sekundarno pogon; potrebna je provjera za pristup podacima pogona.

Kad je pogon postavljen, prozor Samokodirajućeg pogona će nastaviti prikazivati pogon(e) i vezu za korisnika tako da promijeni svoju zaporku pogona. Ako ste administrator pogona, također ćete moći dodati ili ukloniti korisnike pogona iz ovog prozora. Ako postoji vanjski pogon koji je postavljen, prikazivat će se u ovom prozoru i može ga se otključati.

NAPOMENA: Za zaključavanje sekundarnog, vanjskog pogona, pogon se mora isključiti neovisno od računala.

Administrator pogona može upravljati postavkama pogona pod **Naprednim>uređajima**. Za više informacija, pogledajte Upravljanje uređajima - samokodirajući uređaji.

Instalacija pogona

Čarobnjak instalacije samokodirajućeg pogona će vas voditi kroz podešavanje vaših pogona. Važno je imati na umu sljedeće koncepte kad se prolazi kroz ovaj postupak.

Administrator pogona
Prvi korisnik s pravima administratora sustava koju podesi pristup pogonu (o podesi zaporku administratora pogona) postaje administrator pogona; to je jedini korisnik s pravima da unosi promjene pristupu pogonu. Da bi se osiguralo da je prvi korisnik namjerno postavljen kao administrator pogona, morate odabrati potvrdnu kućicu "Razumijem" da biste nastavili s ovim korakom.

Zaporka administratora pogona
Čarobnjak će zatražiti od vas da stvorite zaporku administratora pogona i ponovno unesete zaporku kao potvrdu. Morate unijeti svoju Windows zaporku da biste uspostavili svoj identitet prije nego što možete stvoriti zaporku administratora. Trenutni Windows korisnik mora imati administratorska prava da bi stvorio ovu zaporku.

Izrada sigurnosne kopije akreditacija pogona
Upišite lokaciju ili kliknite tipku **Pregledaj** da biste odabrali lokaciju, da biste spremili sigurnosnu kopiju akreditacija administratora pogona.

VAŽNO**!**

- Preporučuje se da napravite sigurnosne kopije ovih akreditacija i da napravite sigurnosnu kopiju na pogon koji nije vaš primarni tvrdi disk (npr. prijenosni mdiji). Inače, ako izgubite pristup vašem pogonu, nećete moći pristupiti svojoj sigurnosnoj kopiji.
- Kad dovršite instalaciju pogona, svikorisnici će morati unijeti točno korisničko ime i zaporku (ili otisak prsta), prije učitanja sustava Windows, da bi pristupili sustavu sljedeći put kad se uključi.

Dodaj korisnika pogona
Administrator pogona može dodati druge korisnike pogonu, a koji su valjani Windows korisnici. Kod dodavanja korisnika pogonu, administrator ima mogućnost traženja od korisnika da resetira svoju zaporku kod prve prijave. Korisnik će morati resetirati svoju zaporku na zaslonu provjere prije sustava Windows prije otključavanja pogona.

Napredne postavke

- *Jednostruka prijava* - Kao zadano, vaša zaporka samokodirajućeg pogona, koju unesete prije sustava Windows da biste provjerili pogon, će se koristiti za automatsku prijavu i u sustav Windows (to se zove "jednostruka prijava"). Da biste isključili ovu značajku, odaberite potvrdnu kućicu "Želim se ponovno prijaviti kad se pokrene sustav Windows" kod podešavanja postavki vašeg pogona.
- *Prijava otiskom prsta* - Na podržanim platformama, možete odrediti da želite provjeriti da vaš samokodirajući pogon koristi otisak prsta umjesto zaporke.
- *Pasivni način rada/čekanje (S3) pasivni način rada/čekanje* (ako je podržano na platformi) - Ako je uključena, vaš samokodirajući pogon se može sigurno staviti u Pasivni način rada/čekanje (također se naziva S3 način rada) i bit će potrebna prijava prije sustava Windows kod nastavljanja iz Pasivnog načina rada/čekanja.

NAPOMENE:

- Kad je uključena podrška za S3, zaporke kodiranja pogona su podložne svim postojećim ograničenima BIOS zaporke. Konzultirajte se s proizvođačem hardvera sustava za više informacija o svim specifičnim ograničenjima zaporki BIOS-a koje mogu postojati u sustavu.
- Ne podržavaju svi samokodirajući pogoni S3 način rada. Tijekom instalacije pogona, bit ćete obaviješteni o tome da li pogon podržava pasivni režim/čekanje. Za pogone koji ne podržavaju ovaj način rada, zahtjevi Windows S3 će se automatski pretvoriti u zahtjeve za hibernacijom, ako je uključen hibernacijski način rada (preporučujemo da uključite hibernacijski način rada na vašem računalu).
- Prvi put kad se prijavite nakon postavljanja opcije jednostruke prijave, postupak će se zaustaviti na upitu prijave na sustav Windows. Morat ćete unijeti oblik provjere za sustav Windows, koja će biti sigurno spremljena za buduće pokušaje prijave na sustav Windows. Idući put kad se učita sustav, SSO će vas automatski prijaviti na sustav Windows. Isti postupak je također potreban kad se promijeni provjera korisnika za sustav Windows (zaporka, otisak prsta, PIN pametne kartice). Ako je računalo na domeni, a ta domena ima smjernice koje traže da se ctrl+alt+del pritisne nakon prijave na sustav Windows, ove smjernice će se poštovati.

PAŽNJA! Ako deinstalirate aplikaciju **Dell Data Protection | Access**, morate prvo isključiti zaštitu podataka samokodirajućeg pogona i otključati pogon.

Korisničke funkcije samokodirajućeg pogona

Administratori samokodirajućeg pogona mogu u potpunosti upravljati sigurnošću pogona i korisnicima. Korisnici pogona koji nisu administrator pogona mogu obavljati samo sljedeće zadaće:

- Promijeniti svoje zaporke pogona
- Otključati pogon

Ovim se zadaćama može pristupiti s pločice **Samokodirajući pogon** u **Dell Data Protection | Access**.

Promijeni zaporku
Ovo omogućava prijavljenim korisnicima da stvore svoju novu zaporku za provjeru pogona. Morate unijeti svojuzaporku samokodirajućeg pogona prije ppostavljanja zaporke pogona na novu vrijednost.

NAPOMENE:

- Ova će aplikacija nametnuti duljinu Windows zaporke i smjernice o složenosti zaporke, ako su uključene. Ako smjernice o zaporki sustava Windows nisu uključene, maksimalna duljina zaporke samokodirajućeg pogona je 32 znaka. Imajte na umu da je maksimalna duljina 127 znakova ako nije uključenS3 (Pasivni režim/čekanje) .
- Zaporka korisnika samokodirajućeg pogona je različita od njihove Windows zaporke. Kada se promijeni Windows zaporka korisnika ili se resetira, to nema utjecaja na korisnikovu zaporku za pogon, osim ako je uključena Windows sinkronizacija zaporke. Za detaljne informacije, pogledajte Uređaji: Samokodirajući pogoni za detaljne informacije.
- Na nekim neengleskim tipkovnicama, postoji niz zabranjenih znakova koje se ne mogu koristiti za zaporku samokodirajućeg pogona. Ako Windows zaporka sadrži bilo koji od ograničenih znakova, a Windows sinkronizacija zaporki je uključena, sinkronizacija neće uspjeti i doći će do poruke o pogrešci.

Otključavanje pogona
Otključavanje pogona omogućava prijavljenom pogonu da otključa zaključani pogon. Ako je zaključavanje pogona uključeno, pogon ulazi u zaključano stanje kad god se isključi napajanje računala. Kad se napajanje sustava vrati, morate se prijaviti na pogon tako da unesete zaporku na zaslon provjere prije sustava Windows.

NAPOMENE:

- Može doći do nemogućnosti ulaska u režim uštede energije (tj. režim na čekanju/pasivni ežim) ako je više korisničkih računa za samokodirajući pogon istodobno prijavljeno na računalo.
- Na zaslonu provjere prije sustava Windows, "Korisnik 1", "Korisnik 2" itd se zamjenjuju imenima korisnika pogona u inačicama aplikacije koje su lokalizirane na sljedećim jezicima: kineski, japanski, korejski i ruski jezik.

Napredne mogućnosti

Napredne mogućnosti u **Dell Data Protection | Access** omogućavaju korisniku s administratorskim ovlastima da upravlja sljedećim aspektima aplikacije:

Maintenance (Održavanje)
Zaporke
Uređaji

NAPOMENA: Samo korisnici s administratorskim ovlastima mogu unositi izmjene u Naprednim mogućnostima; standardni korisnici mogu vidjeti te postavke ali ih ne mogu mijenjati.

Maintenance (Održavanje)

Prozor Održavanje mogu koristiti administratori da podese mogućnosti prijave na sustav Windows, ponovno pokrenuti sustav da ga pripreme na drugu svrhu ili za arhiviranje ili vraćanje akreditacija korisnika spremljenih u sigurnosnim hardveru sustava. Za detaljne informacije, pogledajte sljedeće teme:

Svojstva pristupa
Ponovno pokreni sustav
Arhiva akreditacija & vrati

Svojstva pristupa

Prozor svojstva pristupa omogućava administratorima da odrede svojstva prijave na sustav Windows za sve korisnike sustava.

Uključi Dell Secure login
Mogućnost zamjene standardnog ctrl-alt-delete zaslona vam omogućava da koristite različite čimbenike provjere umjesto (ili pored) Windows zaporke za pristuo sustavu Windows. Možete odabrati dodati otisak prsta kao drugi čimbenik provjere da biste pojačali sigurnost procesa prijave na sustav Windows. Dodatni faktori provjere se također mogu dodati za prijavu na sustav Windows, uključujući pametnu karticu ili TPM certifikat.

NAPOMENE:

- Uključivanje Dell Secure login-a utječe na sve korisnike sustava.
- Preporučuje se da je ova opcija uključi NAKON što korisnici prijave svoje otiske prstiju ili pametnu karticu.
- Kad se prvi put prijavite nakon postavljanja ove opcije, tražit će se od vas da izvršite provjeru za sustav Windows prema vašim standardnim smjernicama, i tad ćete morati koristiti nove čimbenike provjere kod sljedećeg učitavanja.

Isključi Dell Secure login
Ova mogućnost isključuje sve funkcije aplikacije **Dell Data Protection | Access** za prijavu na sustav Windows. Kad se to odabere, vratit ćete se na vaše standardne smjernice prijave na sustav Windows.

NAPOMENE:

- ako dobijete pogrešku vezanu za sigurnu prijavu na sustav Windows ako se pokušavate prijaviti, isključite i ponovno uključite mogućnost Dell Secure login.
- Ako želite detaljnije informacije o određenoj poruci pogreške, idite na wave.com/support/Dell.

Ponovno pokretanje sustava

Funkcija ponovnog pokretanja sustava se koristi za brisanje svih korisničkih podataka sa svog sigurnosnog hardvera na platformi; ona se koristi, na primjer, za promjenu namjene računala. Ova opcija briše sve zaporke u sustavu, osim korisničkih zaporki sustava Windows, kao i sve podatke u hardverskim uređajima (tj. ControlVault, TPM i čitačima otiska prsta). Za samokodirajuće pogone, ova funkcija također onemogućava zaštitu podataka tako da se podacima na pogonu može pristupiti.

Morate potvrditi da razumijete da ponovno pokrećete sustav, zatim kliknite na **Dalje**. Da biste ponovno pokrenuli sustav, morat ćete unijeti zaporku za svaki sigurnosni uređaj, ako su postavljene:

- TPM vlasnik
- Administrator ControlVaulta
- Administrator BIOS-a
- BIOS sustav (prije-Windowsa)
- Tvrdi disk (BIOS)
- Administrator samokodirajućeg pogona

NAPOMENA: Za samokodirajuće pogone, potrebna je samo zaporka administratora pogona; nisu potrebne zaporke svih korisnika pogona.

Važno! Jedini način za vraćanje bilo kakvih podataka obrisanih kad ste ponovno pokretali sustav je vraćanje iz prethodno spremljenog arhiva. Ako nemate arhivu, ovi se podaci ne mogu vratiti. Za samokodirajuće pogone, brišu se samo podaci instalacije; ne brišu se osobni podaci na pogonu.

Arhiva akreditacija & Vrati

Funkcija arhiva akreditacija i vraćanja se koristi za izradu sigurnosnih kopija i vraćanje svih korisničkih akreditacija (informacije za prijavu i kodiranje) spremljenih u ControlVault i Trusted Platform Module (TPM). Sigurnosne kopije ovih podataka su važne kod prenamjene računala ili vraćanje podataka u slučaju hardverskog kvara. U tom slučaju možete jednostavno vratiti sve vaše akreditacije na vaše novo računalo iz spremljene arhivske datoteke.

Možete odabrati da li ćete arhivirati ili vratiti akreditacije za jednog korisnika ili za sve korisnike u sustavu.

Korisničke akreditacije se sastoje od podataka korištenih prije sustava Windows, kao što su prijavljeni otisci prstiju ili podaci pametne kartice i ključeva spremljenih u TPM-u. TPM će stvoriti ključeve kako to traže sigurne aplikacije; na primjer, generiranje digitalnog certifikata će stvoriti ključeve u TPM-u.

NAPOMENA: Da biste odredili da li se TPM ključevi mogu arhivirati preko aplikacije **Dell Data Protection | Access**, pogledajte dokumentaciju sigurne apliakcije. Općenito, podržane su aplikacije za generiranje ključeva koje koriste “Wave TCG-Enabled CSP”.

Arhiviranje akreditacija
Za arhiviranje akreditacija, morate uraditi sljedeće:

- Odrediti da li arhivirate akreditacije za sebe ili za sve korisnike u sustavu.
- Izvršite provjeru sigurnosnom hardveru unošenjem zaporke sustava (prije-Windowsa) , zaporku administratora ControlVaulta i TPM zaporku vlasnika.
- Stvorite zaporku sigurnosnih kopija akreditacija.
- Odredite lokaciju arhive pomoću tipke **Pregledaj** . Lokacija arhiva trebaju biti uklonjivi mediji, kao što je USB flash pogon ili mrežni pogon, da biste se zaštitili od kvara hardvera.

Važne napomene:

- Zabilježite lokaciju arhive jer će korisniku biti potrebne te informacije za vraćanje informacija akreditacija.
- Zabilježite zaporku sigurnosne kopije akreditacija da biste bili sigurni da se podaci mogu vratiti. Ovo je važno jer se ova zaporka ne može vratiti.
- Ako ne znate zaporku TPM vlasnika, javite se administratoru sustava ili pogledajte upute instalacije TPM-a računala.

Vraćanje akreditacija
Za vraćanje akreditacija, morate uraditi sljedeće:

- Odrediti da li vraćate akreditacije za sebe ili za sve korisnike u sustavu.
- Idite na lokaciju arhive i odaberite arhivsku datoteku.
- Unesite zaporku sigurnosne kopije akreditacija koja je stvorena kad ste postavljali arhivu.
- Izvršite provjeru sigurnosnom hardveru unošenjem zaporke sustava (prije-Windowsa) , zaporku administratora ControlVaulta i TPM zaporku vlasnika.

NAPOMENE:

- Ako dobijete pogrešku koja kaže da vraćanje akreditacija nije uspjelo i nekoliko puta niste uspjeli vratiti, pokušajte vratiti drugu datoteku arhive. Ako to nije bilo uspješno, stvorite drugu arhivu akreditacije i pokušajte vratiti iz nove arhive.
- Ako dobijete pogrešku koja navodi da TPM ključevi nisu mogli biti vraćeni, stvorite arhivu akreditacija, zatim obrišite TPM u BIOS-u. Da biste obrišite TPM, ponovno pokrenite vaše

računalo, pritisnite tipku **F2** kad budete počinjali s izradom sigurnosnih kopija za pristup postavkama BIOS-a, zatim idite na Sigurnost>TPM sigurnost. Zatim ponovno uspostavite vlasništvo nad TPM-om i pokušajte ponovno vratiti akreditacije.

- Ako želite detaljnije informacije o određenoj poruci pogreške, idite na wave.com/support/Dell.

Upravljanje zaporkama

Iz prozora Password Management, administrator može stvarati ili mijenjati sve sigurnosne zaporke na vašem sustavu:

- Sustav (također poznato kao prije-Windowsa)*
- Administrator*
- Tvrdi disk*
- ControlVault
- TPM vlasnik
- TPM Master
- TPM Password Vault
- Samokodirajući pogon

NAPOMENE:

- Bit će prikazane samo zaporke koje se mogu primijeniti na trenutnu konfiguraciju platforme; tako će se ovaj prozor mijenjati ovisno o konfiguraciji i statusu sustava.
- Gornje zaporke sa * pored njih su BIOS zaporke i također se migu mijenjati preko sustava BIOS.
- Zaporke na razini BIOS-a se ne mogu stvarati ili mijenjati ako je BIOS administrator zabranio promjene zaporki.
- Klikom na vezu **instalacija** za samokodirajući disk pokreće čarobnjak za instalaciju samokodirajućeg diska; klik na **upravljaj** omogućava korisniku jednu ili više zaporku samokodirajućeg pogona.
- Klikom na vezu **upravljaj**TPM Password Vault-a, prikazat će se prozor u kojem možete vidjeti ili promijeniti zaporke koje štite vaše TPM ključeve. Kad se stvori TMP ključ za koji je potrebna zaporka, zaporka se generira nasumično i stavlja u spremnik. Ne možete upravljati TPM Password Vault-om dok ne stvorite TPM glavnu zaporku.

Pravila složenosti zaporke sustava Windows

Dell Data Protection | Access osigurava da je sljedeća zaporka u skladu sa sustavom Windows pravila složenosti zaporke za stroj:

- Zaporka TPM vlasnika

Da biste odredili smjernice složenosti zaporke za sustav Windows, slijedite ove korake:

1. Pristupite Upravljačkoj ploči
2. Dvaput kliknite na Administrativne alate.
3. dvaput kliknite na Lokalne sigurnosne smjernice.
4. Proširite Smjernice računa i odaberite Smjernice o zaporki.

Uređaji

Prozor Uređaji koriste administratori za upravljanje svim sigurnosnim uređajima instaliranim na njihovom sustavu. Za svaki uređaj možete vidjeti status i dodatne detaljne informacije kao što je inačica ugrađenog softvera. Kliknite na **prikaži** da biste vidjeli informacije za svaki uređaj, ili **sakrij** da spustite taj dio. Uređaji kojima se može upravljati su sljedeći, ovisno tome što vaša platforma sadrži:

Trusted Platform Module (TPM)
ControlVault®
Samokodirajući pogon(i)
Informacije o uređaju za provjeru

Trusted Platform Module (TPM)

TPM sigurnosni čip mora biti omogućen i vasništvo nad TPM-om mora biti uspostavljeno da bi se koristile napredne sigurnosne značajke dostupne s aplikacijom **Dell Data Protection | Access** i TPM-om.

Prozor Trusted Platform Module u **Device Managementu** se prikazuje samo kad je TPM otkriven na vašem sustavu.

Upravljanje TPM-om

Ove funkcije omogućavaju administratoru sustava da upravlja TPM-om.

Status
Prikazuje status *aktivan* ili *neaktivan* za TPM. Status "Aktivan" znači da je TPM omogućen u BIOS-u i spreman je za podešavanje (tj. može se preuzeti vlasništvo). TPM-om se ne može upravljati a njegovim sigurnosnim značajkama se ne može pristupiti ako TPM nije aktivan (uključen).

Ako je TPM otkriven na sustavu ali nije aktivan (omogućen), možete ga omogućiti klikom na vezu **aktiviraj** na ovom prozoru, bez ulaska u sustav BIOS. Nakon uključivanja TPM-a pomoću ove značajke, računalo se mora ponovno pokrenuti. Tijekom ponovnog pokretanja, u nekim će se slučajevima pojaviti upit koji od vas traži da prihvatite promjene.

NAPOMENA: Mogućnost uključivanja (aktiviranja) TPM-a iz ove aplikacije možda nije podržana na svim platformama. Ako nije podržana, morate je omogućiti u sustavu BIOS. Da biste to uradili, ponovno pokrenite sustav, pritisnite tipku **F2** prije učitavanja sustava Windows da biste ušli u BIOS instalaciju, zatim idite na Sigurnost>TPM Sigurnost i uključite TPM.

Možete također *deaktivirati* TPM s ovog mjesta tako da kliknete na vezu **deaktiviraj**; deaktivacija TPM-a će ga učiniti nedostupnim za napredne sigurnosne značajke. Deaktivacija, međutim, ne mijenja bilo koje TPM postavke i ne briše ili mijenja bilo kakve informacije ili ključeve spremljene u TPM-u.

U vlasništvu
Prikazuje status vlasništva (tj. "u vlasništvu") i omogućava vam da uspostavite ili promijenite TPM vlasnika. TPM vlasništvo se mora uspostaviti zbog da bi njegove sigurnosne značajke bile dostupne. Prije uspostavljanja vlasništva, TPM mora biti uključen (aktiviran).

Postupak za uspostavu vlasništva se sastoji od toga da korisnih (s administratorskim ovlastima) stvori TPM zaporku vlasnika. Kad se ta zaporka definira, vlasništvo se uspostavlja i TPM je spreman za uporabu.

NAPOMENA: The TPM zaporka vlasnika mora udovoljavati pravilima složenosti zaporke sustava Windows za vaš sustav.

Važno! Važno je da ne izgubite ili zaboravite TPM zaporku vlasnika jer je potrebna za pristup naprednim sigurnosnim funkcijama za TPM u **Dell Data Protection | Access**.

Zaključano
Prikazuje status *zaključan* ili *otključan* za TPM. "Zaključavanje" je sigurnosna značajka TPM-a; TPM će ući u zaključano stanje nakon određenog broja netočnih unosa TPM zaporke vlasnika. TPM vlasnik može otključati TPM od tamo; potreban je unos TPM zaporke vlasnika.

NAPOMENE:

- Ako dobijete pogrešku koja kaže da vlasništvo nad TPM-om nije bilo moguće uspostaviti, obrišite TPM u sustavu BIOS i pokušajte ponovno uspostaviti vlasništvo. Da biste obrisali TPM, ponovno pokrenite vaše računalo, pritisnite tipku **F2** kad budete počinjali s izradom sigurnosnih kopija za pristup postavkama BIOS-a, zatim idite na Sigurnost>TPM sigurnost.
- Ako dobijete pogrešku koja navodi da se TPM zaporka vlasnika nije mogla promijeniti, arhivirajte TPM podatke (arhiva akreditacija), očistite TPM u BIOS-u, ponovno uspostavite vlasništvo nad TPM-om i vratite TPM podatke (vratite akreditacije).
- Ako želite detaljnije informacije o određenoj poruci pogreške, idite na wave.com/support/Dell.

Dell ControlVault®

The Dell ControlVault® (CV) je sigurnosni hardverski spremnik za akreditaciju korisnika koji se koristi prije prijave na sustav Windows (npr. korisničke zaporke ili podatke o prijavljenim otiscima prsta). Prozor ControlVault u **Device Managementu** se prikazuje samo kad je ControlVault otkriven na vašem sustavu.

Upravljanje ControlVaultom

Ove funkcije omogućavaju administratoru sustava da upravlja ControlVault-om sustava.

Status
Prikazuje status *aktivan* ili *neaktivan* za ControlVault. Status "Neaktivan" znači da ControlVault nije dostupan za pohranu na vašem sustavu. Pogledajte dokumentaciju Dell sustava da biste odredili da li sustav sadrži a ControlVault.

Password (zaporka)
Označava da li je zaporka administratora ControlVaulta postavljena i omogućava vam postavljanje zaporke ili promjenu zaporke (ako je već postavljena). Samo administratori sustava mogu postaviti ili promijeniti zaporku. Zaporka administratora ControlVaulta se mora postaviti da bi se uradilo sljedeće:

- Izvršite arhiviranje ili vraćanje akreditacija.
- Obriši korisničke podatke (za sve korisnike).

NAPOMENA: Ako se arhiviranje ili vraćanje pokušaju kad zaporka administratora ControlVaulta nije postavljena, od njega/nje se traži da je stvore (ako su administrator).

Prijavljeni korisnici
Označava da li bilo koji korisnik ima prijavljene akreditacije za prijavu (npr. zaporke, otisak prsta ili podatke pametne kartice) koje su trenutno spremljene u ControlVaultu.

Brisanje korisničkih podataka
Podaci u ControlVaultu se moraju u jednom trenutku očistiti; na primjerm ako korisnici imaju problema s uporabom ili prijavom akreditacija prije sustava Windows za provjeru. Iz ovog prozora se mogu obrisati svi podaci spremljeni u ControlVaultu, za jednog korisnika ili za sve korisike.

Zaporka administratora ControlVaulta se mora unijeti da bi se obrisali svi korisnički podaci na platformi. Također će se od vas tražiti zaporka sustava (prije sustava Windows) ako su prijavljene bilo kakve akreditacije prije sustava Windows. Kad obrišete sve korisničke podatke, zaporka administratora ControlVaulta i zaporke sustava se resetiraju; imajte na umu da je to jedini način za brisanje zaporke administratora ControlVaulta.

NAPOMENA: Jednom kad obrišete sve korisničke podatke, od vas će se tražiti da ponovno pokrenete svoje računalo. Važno je da ponovno pokrenete sustav zbog njegovog pravilnog funkcioniranja.

Zaporka administratora ControlVaulta se ne mora postaviti da bi se obrisale akreditacije jednog korisnika. Kad kliknete na **obriši podatke o korisniku**, od vas se traži da odaberete korisnika čije akreditacije ControlVaulta želite obrisati. Kad odaberete korisnika, od vas će se tražiti zaporka sustava (samo ako su prijavljene akreditacije prije sustava Windows).

NAPOMENE:

- Ako dobivate pogrešku koja kaže da se zaporka administratora ControlVaulta ne može stvoriti, morate arhivirati akreditacije, obrisati sve korisničke podatke iz ControlVaulta, ponovno pokrenuti računalo i ponovno pokušati stvoriti zaporku.

- Ako dobivate pogrešku koja navodi da se akreditacije ne mogu obrisati iz ControlVaulta za jednog korisnika, trebate arhivirati akreditacije, pokušati obrisati sve korisničke podatke i tada ponovno pokušati obrisati podatke za tog jednog korisnika.
- Ako dobijete pogrešku koja kaže da akreditacije nisu mogle biti obrisane iz ControlVaulta za sve korisnike, trebate pokušati s ponovnim pokretanjem sustava. **Važno!** Pregledajte teme pomoći o ponovnom pokretanju sustava prije obavljanja ponovnog pokretanja, jer će to obrisati SVE sigurnosne podatke korisnika.
- ako dobijete pogrešku koja navodi da se za ControlVault i TPM nisu moge napraviti sigurnosne kopije, isključite TPM u sustavu BIOS. To se radi tako da ponovno pokrenite vaše računalo, pritisnite tipku **F2** kad budete počinjali s izradom sigurnosnih kopija za pristup postavkama BIOS-a, zatim idite na Sigurnost>TPM sigurnost. Zatim ponovno uključite TPM i pokušajte ponovno arhivirati svoje podatke ControlVault-a.
- Ako želite detaljnije informacije o određenoj poruci pogreške, idite na wave.com/support/Dell.

Samokodirajući pogoni: Napreno

Dell Data Protection | Access upravlja hardverski zasnovanim sigurnosnim funkcijama samokodirajućih pogona, koji imaju kodiranje podataka uključene u hardver pogona. Ovo upravljanje se koristi da bi se osiguralo da samo ovlašteni korisnici mogu pristupiti kodiranim podacima kad je uključeno zaključavanje pogona.

Prozor samokodirajućeg pogona u **Device Managementu** se prikazuje samo kad je jedan ili više samokodirajućih pogona (SED) prisutno u vašem sustavu.

Važno! Kad je pogon postavljen, zaštita podataka samokodirajućeg pogona i zaključavanje pogona su "uključeni".

Upravljanje pogonom

Ove funkcije omogućavaju administratoru pogona da upravlja postavkama sigurnosti pogona. Promjene postavki sigurnosti pogona se primjenjuju nakon isključenja pogona.

Zaštita podataka

Prikazuje status *uključeno* ili *isključeno* za zaštitu podataka samokodirajućeg pogona. Status "uključen" znači da je sigurnost pogona postavljena; međutim, dok se ne uključi *zaključavanje* pogona, korisnici neće morati izvršiti provjeru prije sustava Windows za pristup.

Na ovom mjestu možete isključiti zaštitu podataka samokodirajućeg pogona. Kad je isključena, sve napredne sigurnosne funkcije samokodirajućeg pogona su isključene a pogon djeluje kao standardni pogon. Isključivanjem zaštite podataka se također brišu sve sigurnosne postavke, uključujući sve akreditacije administratora pogona i korisnika pogona. Ova funkcija, međutim, ne mijenja i ne uklanja bilo kakve podatke o korisniku na pogonu.

Zaključavanje

Prikazuje status *uključeno* ili *isključeno* za zaštitu podataka samokodirajućeg pogona. Pogledajte temuSamokodirajući pogon za informacije o ponašanju zaključanog pogona.

Može biti potrebno privremeno isključiti zaključavanje pogona, što možete uraditi s ovog mjesta. To se ne preporučuje jer akreditacije nisu potrebne za pristup pogonu kad je zaključavanje pogona isključeno, tako da bilo koji korisnik platforme može pristupiti podacima pogona. Isključivanjem zaključavanja pogona se nebrišu bilo kakve sigurnosne postavke, uključujući akreditacije administratora pogona i korisnika pogona ili bilo kakvih podataka o korisniku na pogonu.

PAŽNJA!Ako deinstalirate aplikaciju **Dell Data Protection | Access**, morate prvo isključiti zaštitu podataka samokodirajućeg pogona i otključati pogon.

Administrator pogona

Prikazuje trenutnog administratora pogona. Administrator pogona može s ovog mjesta promijeniti koji je korisnik administrator pogona. Novi administrator mora biti valjani korisnik sustava Windows na sustavu s administratorskim ovlastima. Može biti samo jedan administrator u sustavu.

Korisnici pogona

Prikazuje prijavljene korisnike pogona i broj trenutno prijavljenih korisnika. Maksimalni broj podržanih korisnika je zasnovan na samokodirajućem pogonu (trenutno 4 korisnika za Seagate pogone i 24 za Samsung pogone).

Sinkr.Windows zaporke

Značajka sinkronizacije Windows zaporke (WPS) automatski postavlja da zaporke korisnika samokodirajućeg pogona budu iste kao njihove Windows zaporke. Ova funkcija se ne primjenjuje na administratora pogona; primjenjuje se samo na korisnike pogona. WPS funkcija se može koristiti samo u poslovnim okruženjima u kojima se zaporke moraju primijeniti u određenim vremenskim intervalima (npr. svakih 90 dana); s uključenom ovom opcijom, sve zaporke samokodirajućeg pogona će biti ažurirane automatski kad se promijene ove Windows zaporke.

NAPOMENA: Kad je uključena Windows sinkronizacija zaporke (WPS), korisnikova zaporka samokodirajućeg pogona se ne može promijeniti, njihova se Windows zaporka mora promijeniti da bi se automatski ažurirala zaporka pogona.

Zapamti zadnje korisničko ime

Kad je uključena ova opcija, zadnje uneseno korisničko ime će biti prikazano kao zadano u polju **Korisničko ime**zaslona provjere prije sustava Windows.

Odabir korisničkog imena

Kad je uključena ova opcija, korisnici mogu vidjeti sva korisnička imena pogona u polju **Korisničko ime** zaslona provjere prije sustava Windows.

Kriptografsko brisanje

Ova se opcija može koristiti za "brisanje" svih podataka na samokodirajućem pogonu. To ne briše podatke stvarno, ali briše ključeve koji se koriste za kodiranje podataka, čineći tako podatke beskorisnima. Nema načina za vraćanje podataka pogona nakon kriptografskog brisanja; također, zaštita samokodirajućeg pogona je isključena i pogon je spreman za prenamjenu.

NAPOMENE:

- Ako dobijete bilo kakve greške vezane za funkcije upravljanja samokodirajućim pogonom, potpuno isključite računalo (nemojte ponovno pokrenuti) i ponovno pokrenite.
- Ako želite detaljnije informacije o određenoj poruci pogreške, idite na wave.com/support/Dell.

Informacije o uređaju za provjeru

Prozor Informacije o uređaju za provjeru pod **Upravljanje uređajima** prikazuje informacije i status za sve spojene uređaje za provjeru (tj. čitač otisaka prsta, tradicionalni ili bezkontaktni čitač pametne kartice) na sustavu.

Tehnička podrška

Tehnička podrška za softver **Dell Data Protection | Access** se može pronaći na http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP

Kriptografski davatelj usluga (CSP) s uključenim Wave Systems Trusted Computing Groupom (TCG) je sadržan u aplikaciji **Dell Data Protection | Access** te je dostupan za uporabu kad god je potreban CSP – pozvan izravno iz aplikacije ili se može odabrati s popisa instaliranih CSP-a. Kad god je moguće, izaberite "Wave TCG-Enabled CSP" da biste osigurali da TPM generira ključeve u da njihovim zaporkama upravlja **Dell Data Protection | Access**.

Wave Systems TCG-Enabled CSP-om omogućava aplikacijama da koriste funkcije koje su dostupne na platformama usklađenim s TCG izravno preko MSCAPI-ja. Upravo MSCAPI CSP modul s pojačanim TCG daje funkciju asimetričnog ključa na TPM-u i povećava poboljšanu sigurnost koju daje TPM, bez obzira na specifične zahtjeve dobavljača vezano za davatelja Trusted Software Stack (TSS).

NAPOMENA: Ako je TPM ključevima koje generira Wave TCG-Enabled CSP potrebna zaporka a korisnik je stvorio TPM glavnu zaporku, pojedinačne zaporke ključeva će biti nasumično generirane i spremljene u TPM Password Vault.