Domovská stránka Dell Data Protection | Access

Domovská stránka **Dell Data Protection | Access** je počiatočným prístupovým bodom k funkciám tejto aplikácie. Z tohto okna máte prístup k týmto akciám:

Sprievodca prístupom k systému
Možnosti prístupu
Jednotka s automatickým šifrovaním
Rozšírené možnosti

V pravom dolnom rohu okna je odkaz **Rozšírené**, pomocou ktorého môžete zobraziť rozšírené nastavenia.

Z okna rozšírené možnosti sa môžete kliknutím na odkaz **domov** v pravom dolnom rohu vrátiť na domovskú stránku.

Sprievodca prístupom k systému

Sprievodca prístupom k systému sa automaticky spustí pri prvom spustení aplikácie **Dell Data Protection | Access**. Tento sprievodca vás prevedie nastavením všetkých aspektov zabezpečenia vášho systému vrátane nastavení, ako (napr. iba s použitím hesla alebo s použitím otlačku prstu a hesla) a kedy (pred spustením systému Windows, pri spustení alebo v oboch prípadoch) má prihlásenie k systému prebiehať. Ak má váš systém navyše jednotku s automatickým šifrovaním, môžete ju nakonfigurovať pomocou tohto sprievodcu.

Funkcia správcu

Používatelia s oprávnením správcu systému Windows majú právo používať v aplikácii **Dell Data Access | Protection** nasledujúce funkcie, ktoré štandardní používatelia používať nemôžu:

- Nastavenie / zmena systémového hesla (pred systémom Windows)
- Nastavenie / zmena hesla pevného disku
- Nastavenie / zmena hesla správcu
- Nastavenie / zmena hesla vlastníka čipu TPM
- Nastavenie / zmena hesla správcu ControlVault
- Reset systému
- Archivácia a obnovenie údajov
- Nastavenie / zmena kódu PIN správcu kariet Smartcard
- Vymazanie / reset karty Smartcard
- Povolenie / zakázanie zabezpečeného prihlásenia Dell do systému Windows
- Nastavenie zásad prihlásenia do systému Windows
- Správa jednotiek s automatickým šifrovaním:
    - Povolenie / zakázanie zamykania jednotky s automatickým šifrovaním
    - Povolenie / zakázanie synchronizácie hesla Windows (WPS)
    - Povolenie / zakázanie jednotného prihlásenia (SSO)
    - Vykonanie kryptografického vymazania

Vzdialená správa

Vaša organizácia si môže vytvoriť prostredie, v ktorom je možné centrálne spravovať bezpečnostné funkcie aplikácie **Dell Data Protection | Access** na viacerých platformách (tj. vzdialená správa). funkcií V takom prípade je možné použiť bezpečnostnú infraštruktúru systému Windows (napríklad Active Directory) na bezpečnú správu konkrétnych funkcií aplikácie **Dell Data Protection | Access**.

Ak je počítač vzdialene spravovaný (tj. „vo vlastníctve“ vzdialeného správcu), miestna správa funkcií aplikácie **Dell Data Protection | Access** bude znemožnená a okná pre správu aplikácie nebudú lokálne prístupné. Vzdialene je možné spravovať tieto funkcie:

- Trusted Platform Module (TPM)
- ControlVault
- Prihlásenie pred spustením systému Windows
- Reset systému
- Heslá systému BIOS
- Zásady prihlasovania do systému Windows
- Jednotky s automatickým šifrovaním
- Registrácia otlačkov prstov a kariet Smartcard

Ďalšie informácie o používaní serveru EMBASSY® Remote Administration Server (ERAS) spoločnosti Wave Systems na vzdialenú správu získate od svojho predajcu spoločnosti Dell alebo na adrese dell.com.

Možnosti prístupu

V okne Možnosti prístupu môžete nastavovať spôsob získavania prístupu do systému.

Ak máte nastavené možnosti aplikácie **Dell Data Protection | Access**, zobrazia sa na domovskej stránke medzi dostupnými možnosťami (napr. zmeniť heslo prihlásenia pred spustením systému Windows) K dispozícii máte skratky, ktoré vás po kliknutí prenesú do príslušného okna pre vykonanie konkrétnej akcie (napr. zmena hesla prihlásenia pred spustením systému Windows alebo registrácia nového otlačku prstu).

Všeobecné
Najskôr máte možnosť určiť, kedy sa má uskutočniť prihlásenie (pred spustením systému Windows, po spustení alebo v obidvoch prípadoch) a ako (napr. otlačok prstu a heslo). Môžete zvoliť jednu alebo dve možnosti spôsobu pripojenia – napríklad kombinácia otlačku prstu, karty Smartcard a hesla. Uvedené možnosti sú založené na zásadách prihlasovania používaných vo vašom prostredí a na podpore platformy.

Otlačok prstu
Pokiaľ systém obsahuje čítač otlačkov prstov, môžete registrovať a aktualizovať otlačky prstov, ktoré sa použijú na prihlásenie do systému. Po zaregistrovaní otlačkov prstov môžete prejdením zaregistrovaného prsta cez čítač otlačkov získať prístup do systému v prihlásení pred alebo po spustení systému Windows, či v oboch prípadoch (v závislosti od nastavení všeobecných možností prístupu). Ďalšie informácie nájdete v časti Registrácia používateľských otlačkov prstov.

Prihlásenie pred spustením systému Windows
Ak ste sa rozhodli, že sa používatelia musia prihlasovať pred spustením systému Windows, je potrebné nastaviť systémové heslo (nazývané tiež heslo pred spustením systému Windows) na spustenie systému Windows. Po vytvorení tohto hesla ho môže správca kedykoľvek zmeniť.

Na tejto obrazovke môžete prihlásenie pred spustením systému Windows tiež zakázať – je potrebné zadať aktuálne systémové heslo, potvrdiť jeho správnosť a potom kliknúť na tlačidlo **Zakázať**.

Karta Smartcard
Ak ste rozhodli, že používatelia musia pri prihlásení používať kartu Smartcard, je potrebné zaregistrovať jednu alebo viac tradičných (s kontaktami) alebo bezkontaktných kariet Smartcard. Kliknutím na odkaz **Zaregistrovať ďalšiu kartu Smartcard** spustíte sprievodcu registráciou kariet Smartcard. Registrácia znamená nastavenie karty Smartcard na použitie pre prihlásenie.

Po zaregistrovaní karty Smartcard môžete nastaviť alebo zmeniť kód PIN tejto karty pomocou odkazu **Nastaviť alebo zmeniť kód PIN karty Smartcard**.

Prihlásenie pred spustením systému Windows

Ak je nastavené prihlásenie pred spustením systému Windows, overenie (heslo, otlačok prstu alebo karta Smartcard) sa vyžaduje po spustení systému ešte pred tým, ako sa spustí systém Windows. Funkcia prihlásenia pred spustením systému Windows poskytuje systému dodatočné zabezpečenie tak, že bráni neoprávneným používateľom pri vstupe do systému Windows a pri prístupe k počítaču (napr. v prípade krádeže).

V okne Prihlásenie pred spustením systému Windows môžu správcovia prihlásenia nastavovať a vytvárať či meniť heslo pred spustením systému Windows (systémové). Pokiaľ je heslo už nastavené, v tomto okne môžete prihlásenie pred spustením systému Windows deaktivovať. Nastavenie prihlásenia pred spustením systému Windows spustí sprievodcu, ktorý vykoná nasledujúce akcie:

- Systémové heslo: Nastavenie systémového hesla (heslo pred spustením systému Windows) pre prístup pred spustením systému Windows. Toto heslo sa používa aj ako záloha pre prípad, keď má používateľ dodatočné faktory overovania (napr. aby bolo možné získať prístup do systému v prípade, že dôjde k problému s čítačom otlačkov prstov.).
- Otlačok prstu a karta Smartcard: Nastavte otlačok prstu alebo kartu Smartcard na použitie pre prihlásenie pred spustením systému Windows a určite, či má byť tento faktor overovania použitý ako náhrada hesla alebo ako jeho doplnok.
- Jednotné prihlásenie: Štandardne bude vaše overenie pred spustením systému Windows (heslo, otlačok prstu alebo karta Smartcard) použité tiež na automatické prihlásenie do systému Windows (to sa nazýva „Jednotné prihlásenie“). Túto funkciu zrušíte začiarknutím políčka „Zachovať prihlásenie v systéme Windows“.
- Pokiaľ by okrem hesla pred spustením systému bolo nastavené tiež heslo pevného disku systému BIOS, máte tiež možnosť zmeniť alebo zrušiť heslo pevného disku.

POZNÁMKA: Nie všetky čítače otlačkov prstov je možné použiť pre overenie pred spustením systému Windows. Pokiaľ váš čítač nie je kompatibilný, môžete registrovať otlačky prstov iba pre prihlásenie do systému Windows. Informácie o kompatibilných čítačoch otlačkov prstov získate od správcu systému alebo na adrese support.dell.com, kde nájdete zoznam podporovaných čítačov otlačkov.

Deaktivácia prihlásenie pred spustením systému Windows
V tomto okne môžete prihlásenie pred spustením systému Windows tiež zakázať– je potrebné zadať aktuálne heslo pred spustením systému Windows (systémové), potvrdiť, že je heslo správne, a potom kliknúť na tlačidlo **Zakázať**. Ak zakážete prihlásenie pred spustením systému Windows, zaregistrované otlačky prstov a karty Smartcard ostanú zaregistrované.

Registrácia otlačkov prstov

Používatelia sa pri overení systémom pri alebo pred spustením systému Windows môžu registrovať alebo aktualizovaťotlačkami prstov. Na karte Otlačky prstov sú obrázky rúk, ktoré zobrazujú, ktoré prsty boli zaregistrované. Po kliknutí na odkaz **Zaregistrovať ďalšie** sa spustí sprievodca registráciou otlačkov prstov, ktorá vás prevedie celým procesom registrácie. „Registrácia“ znamená uloženie otlačku prsta na použitie pri prihlásení. Aby bola registrácia možná, musí byť správne nainštalovaný a nakonfigurovaný čítač otlačkov prstov.

POZNÁMKA: Nie všetky čítače otlačkov prstov je možné použiť na prihlásenie pred spustením systému Windows. Ak sa pomocou nekompatibilného čítača pokúsite zaregistrovať otlačky na prihlásenie pred spustením systému Windows, zobrazí sa chybová správa. Informácie o kompatibilných zariadeniach získate od správcu systému a na adrese support.dell.com nájdete zoznam podporovaných čítačov otlačkov.

Pri registrácii otlačku prsta budete vyzvaní na overenie vašej identity zadaním hesla systému Windows. Ak to to vaše zásady vyžadujú, budete vyzvaní tiež na zadanie hesla pred spustením systému Windows (systémového). Heslo pred spustením systému Windows je možné použiť na získanie prístupu do systému v prípade, že nastane problém s čítačom otlačkov prstov.

POZNÁMKY:

- Odporúča sa počas procesu registrácie zaregistrovať aspoň dva otlačky prstov.
- Pred aktiváciou overenia pomocou otlačkov prstov je potrebné zaistiť, aby boli otlačky prstov riadne zaregistrované.
- Ak v systéme vymeníte čítač otlačkov, je otlačky prstov potrebné zaregistrovať s týmto novým čítačom. Prepínanie medzi dvomi rôznymi čítačmi otlačkov prstov sa neodporúča.
- Ak sa vám pri registrácii otlačkov prstov opakovane zobrazuje správa „snímač stratil zaostrenie“, je možné, že počítač čítač otlačkov prstov nerozpoznáva. Ak používate externý čítač otlačkov, v mnohých prípadoch problém vyriešite jeho odpojením a opätovným pripojením.

Vymazanie registrovaných otlačkov prstov
Zaregistrované otlačky prstov môžete odobrať kliknutím na odkaz **Odobrať otlačok prstu** alebo kliknutím na zaregistrovaný prst (zrušením výberu) v sprievodcovi registráciou otlačkov prstov.

Konkrétneho používateľa s otlačkami prstov zaregistrovaného pre overenie pred spustením systému Windows môže správca odobrať zrušením výberu všetkých otlačkov prstov zaregistrovaných týmto používateľom.

POZNÁMKA: Ak počas registrácie otlačkov prstov nastanú chyby, ďalšie podrobnosti nájdete na adrese wave.com/support/Dell.

Registrácia kariet Smartcard

Dell Data Protection | Access umožňuje používať tradičné (s kontaktami) alebo bezkontaktné karty Smartcard na prihlásenie k účtu systému Windows alebo k overeniu pred spustením systému Windows. Na karte Smartcard kliknutím na odkaz **Zaregistrovať ďalšiu kartu Smartcard** spustite sprievodcu registráciou karty Smartcard, ktorý vás prevedie procesom registrácie. „Registrácia“ znamená nastavenie karty Smartcard, aby sa pri prihlásení používala.

Aby bola registrácia možná, musí byť správne nainštalované a nakonfigurované zariadenie na overovanie kariet Smartcard.

POZNÁMKA: Informácie o kompatibilných zariadeniach získate od správcu systému a na adrese support.dell.com nájdete zoznam podporovaných kariet Smartcard.

Registrácia
Pri registrácii karty Smartcard budete vyzvaní na overenie vašej identity zadaním hesla systému Windows. Ak to vyžadujú vaše zásady, budete vyzvaní tiež na zadanie hesla pred spustením systému Windows (systémového). Heslo pred spustením systému Windows je možné použiť na získanie prístupu do systému v prípade, že nastane problém s čítačom kariet Smartcard.

Počas registrácie budete vyzvaní na zadanie kódu PIN karty Smartcard, pokiaľ bol tento nastavený. Ak vaše zásady vyžadujú kód PIN , a žiadny nebol nastavený, budete vyzvaní na jeho vytvorenie.

POZNÁMKY:

- Po zaregistrovaní používateľa na používanie karty Smartcard pre prihlásenie pred spustením systému Windows nie je možné používateľa odobrať.
- Štandardní používatelia môžu meniť používateľský kód PIN karty Smartcard a správca môže meniť ako správcovský, tak aj používateľský kód PIN.
- Správca môže tiež resetovať kartu Smartcard. Po resetovaní kartu Smartcard nie je možné použiť na overenie pri alebo pred spustením systému Windows, pokiaľ nebude znovu zaregistrovaná.

POZNÁMKA: V prípade overovania certifikátov TPM môžu správcovia registrovať certifikáty TPM prostredníctvom procesu registrácie kariet Smartcard systému Microsoft Windows. Aby bola zaistená kompatibilita s touto aplikáciou, správca musí ako poskytovateľa kryptografických služieb zvoliť možnosť „CSP na báze TCG spoločnosti Wave“ namiesto CSP karty Smartcard. Okrem toho sa musí povoliť funkcia zabezpečeného prihlásenia Dell s príslušnou zásadou typu overenia pre klienta.

POZNÁMKA: Pokiaľ sa zobrazí chybová správa, že služba Smartcard nie je spustená, môžete ju spustiť/reštartovať takto:

- Prejdite z Ovládacích panelov do okna Nástroje správy, vyberte položku Služba, kliknite pravým tlačidlom na položku Smartcard a vyberte možnosť Spustiť alebo Reštartovať.
- Podrobnejšie informácie o konkrétnych chybových správach nájdete na adrese wave.com/support/Dell.

Prehľad jednotky s automatickým šifrovaním

Aplikácia **Dell Data Protection | Access** riadi hardvérové bezpečnostné funkciejednotiek s automatickým šifrovaním, ktoré majú šifrovanie údajov zabudované vo svojom hardvéri. Táto funkcia zabezpečuje, aby mali k šifrovaným údajom prístup iba autorizovaní používatelia (ak je povolené uzamykanie jednotky).

Okno Jednotka s automatickým šifrovaním otvoríte kliknutím na spodnú kartu **Jednotka s automatickým šifrovaním**. Táto karta sa zobrazuje len vtedy, keď sa v systéme nachádza jedna alebo viac jednotiek s automatickým šifrovaním (SED).

Kliknutím na odkaz **Nastavenia** spustíte sprievodcu nastavením jednotky s automatickým šifrovaním. V tomto sprievodcovi môžete vytvoriť heslo správcu jednotky, toto heslo zálohovať a použiť nastavenie šifrovania jednotky. K sprievodcovi nastavením jednotky s automatickým šifrovaním majú prístup iba správcovia systému.

Dôležité! Po nastavení jednotky sú „povolené“ funkcie ochrany údajov a uzamykania jednotky. Ak je jednotka uzamknutá, správa sa takto:

- Jednotka prejde do režimu *zamknutý* pri každom vypnutí jej napájania.
- Jednotka sa nespustí, pokiaľ používateľ nezadá správne používateľské meno a heslo (alebo otlačok prstu) na obrazovke prihlásenia pred spustením systému Windows. Pokiaľ nie je povolené uzamykanie jednotky, údaje v nej sú prístupné všetkým používateľom počítača.
- Jednotka je zabezpečená aj v prípade, že je pripojená ako sekundárna jednotka k inému počítaču – pri pokuse o prístup k údajom na jednotke sa vyžaduje overenie.

Po nastavení jednotky zobrazí okno Jednotka s automatickým šifrovaním jednotky a odkaz pre používateľov, aby si zmenili svoje heslá k jednotkám. Pokiaľ ste správcom jednotky, môžete v tomto okne tiež pridávať a odoberať používateľov jednotiek. Ak je prítomná externá jednotka a bola nastavená, zobrazí sa v tomto okne a je možné ju odomknúť.

POZNÁMKA: Aby bolo možné uzamknúť sekundárnu externú jednotku, musí byť vypnutá nezávisle od počítača.

Správca jednotky môže spravovať nastavenia jednotky v časti **Rozšírené>Zariadenia**. Ďalšie informácie nájdete v časti Správa zariadení – Jednotky s automatickým šifrovaním.

Nastavenie jednotky

Sprievodca nastavením jednotky s automatickým šifrovaním vás prevedie nastavením jednotiek. Počas tohto procesu je dôležité mať na pamäti nasledujúce koncepty.

Správca jednotky

Prvý používateľ s oprávneniami správcu systému, ktorý nastaví prístup k jednotke (a nastaví heslo správcu jednotky), sa stane správcom jednotky. Tento používateľ má ako jediný oprávnenie uskutočniť zmeny prístupu k jednotke. Aby ste potvrdili, že prvý používateľ je úmyselne nastavovaný ako správca jednotky, a bolo možné pokračovať k ďalšiemu kroku, je potrebné začiarknuť políčko „Rozumiem“.

Heslo správcu jednotky

Sprievodca vás vyzve na vytvorenie hesla správcu jednotky a k opätovnému zadaniu tohto hesla pre účely potvrdenia. Než budete môcť vytvoriť heslo správcu jednotky, musíte preukázať svoju identitu zadaním hesla do systému Windows. Aby mohol vytvoriť toto heslo, musí mať aktuálny používateľ systému Windows oprávnenia správcu.

Zálohovanie prihlasovacích údajov jednotky
Zadaním alebo kliknutím na tlačidlo **Prehľadávať** vyberte umiestnenie, do ktorého chcete uložiť záložnú kópiu vašich údajov správcu jednotky.

DÔLEŽITÉ**!**

- Tieto prihlasovacie údaje dôrazne odporúčame zálohovať, a to inam než na primárny pevný disk (napr. na vymeniteľné médium). V opačnom prípade by ste v prípade straty prístupu k jednotke neboli schopní pristupovať ani k zálohe.
- Po dokončení nastavení jednotky budú pri najbližšom spustení systému všetcipoužívatelia musieť pred spustením systému Windows zadať správne používateľské meno a heslo (alebo otlačok prstu).

Pridanie používateľa jednotky
Správca jednotky môže k jednotke pridávať ďalších platných používateľov systému Windows. Pri pridaní používateľa k jednotke má správca možnosť vyžadovať od používateľa resetovanie jeho hesla pri prvom prihlásení. Od používateľa sa bude pred odomknutím jednotky vyžadovať resetovanie hesla na obrazovke overenia pred spustením systému Windows.

Rozšírené nastavenia

- *Jednotné prihlásenie* – Štandardne sa vaše heslo k jednotke s automatickým šifrovaním, ktoré zadávate ako overenie pre jednotku pred spustením systému Windows, použije tiež aj pre automatické prihlásenie do systému Windows (táto funkcia sa nazýva „Jednotné prihlásenie“). Túto funkciu môžete deaktivovať v poli „Chcem sa znovu prihlásiť pri spustení systému Windows“ pri konfigurácii nastavení jednotky.
- *Prihlásenie otlačkom prstu* – Na podporovaných platformách môžete určiť, či chcete pre overenie pre jednotku s automatickým šifrovaním použiť namiesto hesla otlačok prstu.
- *Podpora režimu spánku/pohotovostného režimu (S3)* (pokiaľ je na platforme podporovaný) – Pokiaľ je táto funkcia aktívna, vašu jednotku s automatickým šifrovaním je možné bezpečne uviesť do režimu spánku/pohotovostného režimu (inak tiež režimu S3) a pri obnovení z režimu spánku/pohotovostného režimu sa bude vyžadovať overenie pred spustením systému Windows.

POZNÁMKY:

- Keď je podpora režimu S3 aktívna, heslá šifrovania jednotky podliehajú akýmkoľvek existujúcim nárokom na heslá systému BIOS. Ďalšie informácie o akýchkoľvek konkrétnych existujúcich obmedzeniach pre heslá systému BIOS získate od výrobcu hardvéru systému.
- Nie všetky jednotky s automatickým šifrovaním podporujú režim S3. Počas nastavovania jednotky budete informovaní o tom, či jednotka režim spánku/pohotovostný režim podporuje alebo nepodporuje. V prípade jednotiek, ktoré tento režim nepodporujú, budú požiadavky typu S3 systému Windows automaticky prevádzané na požiadavky na hibernáciu, pokiaľ je režim hibernácie povolený (silne sa odporúča, aby režim hibernácie bol v počítači povolený).
- Pri prvom prihlásení po aktivácii možnosti jednotného prihlásenia (SSO) sa proces pri výzve na prihlásenie do systému Windows zastaví. Budete vyzvaní na prihlásenie do systému Windows vami zvoleným spôsobom, ktorý bude bezpečne uložený pre účely budúceho prihlasovania do systému Windows. Pri ďalšom spustení systému vás funkcia SSO automaticky prihlási do systému Windows. Rovnaký proces sa vyžaduje aj vtedy, keď sa mení overenie používateľa pre systém Windows (heslo, otlačok prstu, kód PIN karty Smartcard). Ak sa počítač nachádza na doméne, ktorá má zásadu vyžadujúcu stlačenie klávesov ctrl+alt+del pred spustením systému Windows, táto zásada sa bude rešpektovať.

POZOR! Ak chcete odinštalovať aplikáciu **Dell Data Protection | Access**, musíte najskôr zakázať ochranu údajov jednotky s automatickým šifrovaním a odomknúť jednotku.

Používateľské funkcie SED

Správcovia jednotiek s automatickým šifrovaním zaistia všetku správu zabezpečenia jednotky a používateľov. Používatelia jednotky, ktorí nie sú jej správcami, môžu vykonávať iba tieto akcie:

- Meniť vlastné heslo k jednotke
- Odomknúť jednotku

Tieto akcie je možné vykonať z karty **Jednotka s automatickým šifrovaním** v aplikácii **Dell Data Protection | Access**.

Zmena hesla
Umožňuje zaregistrovaným používateľom vytvoriť nové overovacie heslo jednotky. Pred nastavením hesla jednotky s automatickým šifrovaním na novú hodnotu je potrebné zadať aktuálne heslo jednotky.

POZNÁMKY:

- Aplikácia si vyžiada dodržanie zásad systému Windows pre dĺžku a zložitosť hesla, pokiaľ sú nastavené. Ak zásady systému Windows pre vytváranie hesiel nie sú nastavené, maximálna dĺžka hesla jednotky s automatickým šifrovaním je 32 znakov. V prípade, že nie je povolený režim S3 (režim spánku/pohotovostný režim), maximálna dĺžka je 127 znakov.
- Heslo používateľa k jednotke s automatickým šifrovaním nie je zhodné s heslom do systému Windows. Pokiaľ sa používateľské heslo k systému Windows zmení alebo resetuje, nemá to vplyv na používateľské heslo jednotky v prípade, že nebola aktivovaná synchronizácia s heslom k systému Windows. Podrobnosti nájdete v časti Zariadenia: Jednotky s automatickým šifrovaním.
- Na niektorých klávesniciach v inom než anglickom jazyku existujú znaky, ktoré nie je možné v hesle jednotky s automatickým šifrovaním použiť. Pokiaľ heslo systému Windows obsahuje niektorý z nižšie uvedených znakov a je povolená synchronizácia s heslom k systému Windows, synchronizácia sa nepodarí a zobrazí sa chybová správa.

Odomknutie jednotky
Odomknutie jednotky umožňuje zaregistrovanému používateľovi odomknúťuzamknutú jednotku. Pokiaľ je povolené uzamykanie jednotky, jednotka prejde do uzamknutého stavu pri každom vypnutí napájania počítača. Pri najbližšom spustení systému je potrebné vykonať overenie pre jednotku zadaním hesla na obrazovke prihlásenia pred spustením systému Windows.

POZNÁMKY:

- Ak je na počítači súčasne aktívnych viac účtov používateľov jednotky s automatickým šifrovaním, nemusí byť možné vstúpenie do úsporného režimu (tj. režimu spánku/pohotovostného režimu či hibernácie).
- Na overovacej obrazovke pred spustením systému Windows sú mená používateľov jednotky nahradené názvami „User 1“, „User 2“ atď. vo verziách aplikácie lokalizovaných do týchto jazykov: Čínština, japončina, kórejčina a ruština.

Rozšírené možnosti

Rozšírené možnosti aplikácie **Dell Data Protection | Access** umožňujú používateľovi s oprávneniami správcu ovládať nasledujúce aspekty aplikácie:

Údržba
Heslá
Zariadenia

POZNÁMKA: Úpravy rozšírených možností môžu vykonávať iba používatelia s oprávneniami správcu; štandardní používatelia si môžu tieto nastavenia prezerať, ale nemôžu vykonávať zmeny.

Údržba

Okno Údržba slúži správcom na nastavenie predvolieb prihlásenia do systému Windows, na obnovenie systému v príprave na zmenu použitia alebo na archiváciu či obnovenie používateľských údajov uložených v bezpečnostnom hardvéri systému. Podrobnosti nájdete v týchto témach:

Predvoľby prístupu
Reset systému
Archivácia a obnovenie údajov

Predvoľby prístupu

Okno Predvoľby prístupu umožňujú správcom nastavovať predvoľby prihlásenia do systému Windows pre všetkých používateľov systému.

Aktivácia zabezpečeného prihlásenia Dell
Možnosť nahradiť štandardnú obrazovku ctrl-alt-delete systému Windows umožňuje použiť rôzne faktory overovania namiesto (alebo pre posilnenie) hesla systému Windows pre prístup do systému Windows. Aby ste posilnili zabezpečenie prihlásenia do systému Windows, môžete ako druhý faktor overovania pridať otlačok prstu. Pri prihlasovaní do systému Windows môžete pridať aj ďalšie faktory overovania vrátane karty Smartcard alebo certifikátu TPM.

POZNÁMKY:

- Povolenie zabezpečeného prihlásenia Dell má vplyv na všetkých používateľov systému.
- Túto možnosť odporúčame aktivovať AŽ POTOM, čo si používatelia zaregistrovali otlačky prstov alebo karty Smartcard.
- Pri prvom prihlásení po nastavení tejto možnosti budete vyzvaní na overenie pre systém Windows podľa vašich štandardných zásad a pri ďalšom spustení bude potrebné použiť nové faktory overovania.

Deaktivácia zabezpečeného prihlásenia Dell
Táto možnosť zakáže všetky funkcie aplikácie **Dell Data Protection | Access** pre prihlásenie do systému Windows. Ak zvolíte túto možnosť, vrátite sa k používaniu štandardných zásad prihlasovania do systému Windows.

POZNÁMKY:

- Ak počas prihlasovania nastane chyba týkajúca sa zabezpečeného prihlásenia k systému Windows, deaktivujte a znovu aktivujte možnosť zabezpečeného prihlásenia Dell.
- Podrobnejšie informácie o konkrétnych chybových správach nájdete na adrese wave.com/support/Dell.

Reset systému

Funkcia Reset systému slúži na vymazanie všetkých používateľských údajov zo všetkého bezpečnostného hardvéru na platforme. Používa sa napríklad pri zmene použitia počítača. Táto možnosť vymaže všetky heslá systému s výnimkou používateľských hesiel systému Windows a tiež všetky údaje v hardvérových zariadeniach (tj. úložisko ControlVault, modul TPM a čítače otlačkov prstov). V prípade jednotiek s automatickým šifrovaním táto funkcia zruší tiež ochranu údajov, takže údaje na jednotke budú prístupné.

Musíte potvrdiť, že si uvedomujete, že resetujete systém, a potom kliknite na tlačidlo **Ďalej**. Aby ste mohli systém resetovať, musíte zadať heslo ku každému bezpečnostnému zariadeniu, ktoré má nastavené:

- Heslo vlastníka TPM
- Heslo správcu ControlVault
- Heslo správcu systému BIOS
- Heslo systému BIOS (pred spustením systému Windows)
- Heslo pevného disku (BIOS)
- Heslo správcu jednotky s automatickým šifrovaním

POZNÁMKA: V prípade jednotiek s automatickým šifrovaním sa vyžaduje iba heslo správcu jednotky, nie heslá všetkých používateľov jednotky.

Dôležité! Jediným spôsobom, ako je možné údaje po resetovaní získať späť, je ich obnovenie z vopred uloženého archívu. Ak ste žiadny archív nevytvorili, sú údaje stratené. V prípade jednotiek s automatickým šifrovaním sú vymazané iba údaje nastavení. Osobné údaje na jednotke sa zachovajú.

Archivácia a obnovenie údajov

Funkcie Archivácia a obnovenie údajov slúžia na zálohovanie a obnovenie všetkých používateľských údajov (prihlasovacích a šifrovacích údajov) uložených v úložisku ControlVault a na čipe TPM (Trusted Platform Module). Zálohovanie týchto údajov je dôležité pri prerozdeľovaní počítačov alebo pre obnovenie údajov v prípade zlyhania hardvéru. V takom prípade môžete jednoducho obnoviť všetky vaše údaje do nového počítača z uloženého súboru archívu.

Môžete archivovať a obnovovať údaje jednotlivých používateľov alebo všetkých používateľov v systéme.

Používateľské údaje obsahujú údaje používané pre prihlásenie pred spustením systému Windows ako registrované otlačky prstov, údaje kariet Smartcard a kľúče uložené v module TPM. Modul TPM vytvára kľúče podľa potreby aplikácií pre zabezpečenie – napríklad pri vytvorení digitálneho certifikátu sa vytvoria kľúče v module TPM.

POZNÁMKA: Informácie o tom, či je možné kľúče TPM archivovať pomocou aplikácie **Dell Data Protection | Access**, nájdete v dokumentácii aplikácie pre zabezpečenie. Vo všeobecnosti sú podporované aplikácie, ktoré pre vytváranie kľúčov používajú „CSP na báze TCG spoločnosti Wave“.

Archivácia údajov
Údaje archivujete takto:

- Zadajte, či chcete archivovať údaje pre seba alebo pre všetkých používateľov v systéme.
- Poskytnite overenie zabezpečovaciemu hardvéru zadaním systémového hesla (pred spustením systému Windows), heslo správcu ControlVault a heslo vlastníka modulu TPM.
- Vytvorte heslo zálohy údajov.
- Určite umiestnenie archívu pomocou tlačidla **Prechádzať**. Umiestnením archívu by malo byť vymeniteľné médium, napr. jednotka USB flash alebo sieťová jednotka, aby bola záloha chránená pre prípad zlyhania pevného disku.

Dôležité poznámky:

- Poznamenajte si umiestnenie archívu, pretože používateľ ho bude potrebovať pri obnove údajov.
- Poznamenajte si heslo zálohy údajov, aby ich bolo možné obnoviť. Tento krok je obzvlášť dôležitý, pretože heslo nie je možné spätne zistiť.
- Ak nepoznáte heslo vlastníka modulu TPM, kontaktujte správcu systému alebo si pozrite pokyny pre nastavenie modulu TPM počítača.

Obnovenie údajov
Údaje obnovíte takto:

- Zadajte, či chcete údaje obnoviť pre seba alebo pre všetkých používateľov v systéme.
- Vyhľadajte umiestnenie archívu a vyberte súbor archívu.
- Zadajte heslo zálohy údajov, ktoré ste zadali pri vytvorení archívu.
- Poskytnite overenie zabezpečovaciemu hardvéru zadaním systémového hesla (pred spustením systému Windows), heslo správcu ControlVault a heslo vlastníka modulu TPM.

POZNÁMKY:

- Ak počas obnovenia údajov dôjde k chybe a obnovenie sa nepodarí ani pri ďalších pokusoch, skúste vykonať obnovenie z iného súboru archívu. Ak sa to nepodarí ani tak, vytvorte iný archív údajov a pokúste sa o obnovenie z neho.

- Ak dôjde k chybe počas obnovovania kľúčov TPM, vytvorte archív údajov a potom vymažte modul TPM v systéme BIOS. Ak chcete vymazať modul TPM, reštartujte počítač, stlačením klávesu **F2** počas spúšťania vstúpte do nastavenia systému BIOS a potom prejdete do časti Security>TPM Security. Tu obnovte vlastníctvo modulu TPM a pokúste sa o obnovenie údajov znovu.
- Podrobnejšie informácie o konkrétnych chybových správach nájdete na adrese wave.com/support/Dell.

Správa hesiel

Z okna Správa hesiel môže správca vytvárať a meniť všetky bezpečnostné heslá v systéme:

- Systémové heslo (pred spustením systému Windows)*
- Heslo správcu*
- Heslo pevného disku*
- Heslo ControlVault
- Heslo vlastníka TPM
- Hlavné heslo TPM
- Heslo schránky hesiel TPM
- Heslo jednotky s automatickým šifrovaním

POZNÁMKY:

- Zobrazené budú iba tie heslá, ktoré sú platné pre aktuálnu konfiguráciu platformy - toto okno sa teda bude meniť v závislosti od konfigurácie a stavu systému.
- Heslá so symbolom * sú heslá systému BIOS a tiež ich je možné meniť prostredníctvom systému BIOS.
- Heslá na úrovni systému BIOS nie je možné vytvárať ani meniť, pokiaľ správca systému BIOS zmeny hesiel zakázal.
- Kliknutím na odkaz **nastavenia** pri jednotke s automatickým šifrovaním spustíte sprievodcu jej nastavením. Po kliknutí na položku **spravovať** môže používateľ zmeniť heslo jednej alebo viacerých jednotiek s automatickým šifrovaním
- Kliknutím na odkaz **spravovať** pri schránke hesiel TPM zobrazíte okno, v ktorom môžete prehliadať a meniť heslá chrániace vaše kľúče TPM. Pri vytvorení kľúča TPM vyžadujúceho vytvorenie hesla sa toto heslo náhodne vygeneruje a umiestni sa do schránky. Schránku hesiel TPM nemôžete spravovať, pokiaľ nevytvoríte hlavné heslo TPM.

Pravidlá komplexnosti hesiel systému Windows

Aplikácia **Dell Data Protection | Access** zabezpečuje, aby nasledujúce heslá boli zhodné s pravidlami komplexnosti hesiel počítača:

- Heslo vlastníka TPM

Ak sa chcete zoznámiť s požiadavkami komplexnosti hesiel daného počítača, postupujte podľa nasledujúcich krokov:

1. Otvorte Ovládací panel.
2. Dvakrát kliknite na položku Nástroje na správu.
3. Dvakrát kliknite na položku Lokálna politika zabezpečenia.
4. Otvorte ponuku Politika kont a vyberte možnosť Politika hesla.

Prehľad zariadení

Okno Zariadenia slúži správcom na správu všetkých bezpečnostných zariadení inštalovaných v systéme. Pri každom zariadení môžete zobraziť stav a ďalšie podrobné informácie, ako napríklad verziu firmvéru. Kliknutím na položku **ukázať** zobrazíte informácie o jednotlivých zariadeniach, alebo môžete danú časť zbaliť kliknutím na položku **skryť**. K spravovateľným zariadeniam patria tieto zariadenia podľa toho, ktoré z nich vaša platforma obsahuje:

Trusted Platform Module (TPM)
ControlVault®
Jednotky s automatickým šifrovaním
Informácie o overovacom zariadení

Trusted Platform Module (TPM)

Bezpečnostný čip TPM musí byť povolený a jeho vlastníctvo musí byť určené, aby bolo možné používať pokročilé funkcie zabezpečenia poskytované aplikáciou **Dell Data Protection | Access** a modulom TPM.

Okno Trusted Platform Module v časti **Správa zariadení** sa zobrazí iba vtedy, keď je modul TPM v systému prítomný.

Správa modulu TPM

Tieto funkcie umožňujú správcovi systému spravovať modul TPM.

Stav

Zobrazí pre modul TPM stav *aktívny* alebo *neaktívny*. Stav „Aktívny“ znamená, že modul TPM je v systéme BIOS povolený a že je pripravený na nastavenie (tj. je možné prijať vlastníctvo). Modul TPM nie je možné spravovať a jeho funkcie zabezpečenia nie je možné používať, pokiaľ nie je aktívny (povolený).

Ak je modul TPM v systéme zistený, ale nie je aktívny (povolený), môžete ho povoliť kliknutím na odkaz **aktivovať** v tomto okne bez toho, že by ste museli vstúpiť do systému BIOS. Po povolení modulu TPM pomocou tejto funkcie sa musí počítač reštartovať. Počas reštartovania sa môže zobraziť výzva na potvrdenie zmien.

POZNÁMKA: Možnosť povolenia (aktivácia) modulu TPM z tejto aplikácie nemusí byť podporovaná na všetkých platformách. Ak nie je podporovaná, je potrebné modul povoliť v systéme BIOS. To vykonáte pomocou reštartovania systému tak, že vstúpite do nastavení systému BIOS stlačením klávesu **F2** pred načítaním systému Windows, prejdete do časti Security>TPM Security a aktivujete modul TPM.

Na tomto mieste môžete modul TPM tiež *deaktivovať* kliknutím na odkaz **deaktivovať**. Deaktiváciou modulu TPM spôsobíte zneprístupnenie pokročilých funkcií zabezpečenia. Deaktivácia však nezmení žiadne nastavenia modulu TPM a nevymaže ani nezmení žiadne údaje ani kľúče uložené v module.

Má vlastníka

Zobrazuje stav vlastníctva (tj. „má vlastníka“) a umožňuje určovať alebo meniť vlastníka modulu TPM. Vlastníctvo modulu TPM sa musí určiť preto, aby bolo možné využívať jeho funkcie zabezpečenia.f Aby bolo možné určiť vlastníctvo, modul TPM musí byť najskôr povolený (aktivovaný).

Proces určenia vlastníctva znamená, že používateľ (s oprávneniami správcu) vytvorí Heslo vlastníka TPM. Po definovaní hesla sa určí vlastníctvo a modul TPM je pripravený na použitie.

POZNÁMKA: Heslo vlastníka TPM musí byť v súlade s pravidlami komplexnosti hesiel systému Windows vo vašom systéme.

Dôležité! Je dôležité, aby ste heslo vlastníka TPM nestratili ani nezabudli, pretože sa vyžaduje pre prístup k pokročilým funkciám zabezpečenia modulu TPM v aplikácii **Dell Data Protection | Access**.

Uzamknuté

Zobrazí pre modul TPM stav *uzamknutý* alebo *odomknutý*. „Uzamykanie“ je funkcia zabezpečenia modulu TPM. Modul TPM prejde do stavu uzamknutia po vopred určenom počte zadaní nesprávneho hesla vlastníka TPM. Vlastník modulu TPM ho tu môže odomknúť. Vyžaduje sa zadanie hesla vlastníka TPM.

POZNÁMKY:

- Pokiaľ dôjde k chybe pri vytváraní vlastníctva modulu TPM, vymažte modul TPM v systéme BIOS a pokúste sa o vytvorenie vlastníctva znovu. Ak chcete vymazať modul TPM, reštartujte počítač, počas spúšťania stlačením klávesu **F2** vstúpte do nastavení systému BIOS a potom prejdite do časti Security>TPM Security.
- Ak dôjde k chybe pri zmene hesla vlastníka TPM, archivujte údaje modulu TPM (archív údajov), vymažte modul v systéme BIOS, obnovte jeho vlastníctvo a obnovte údaje modulu TPM (obnovenie údajov).
- Podrobnejšie informácie o konkrétnych chybových správach nájdete na adrese wave.com/support/Dell.

Dell ControlVault®

Dell ControlVault® (CV) je bezpečné hardvérové úložisko pre používateľské údaje potrebné pri prihlásení pred spustením systému Windows (napr. používateľské heslá a zaregistrované otlačky prstov). Okno ControlVault v časti **Správa zariadení** sa zobrazí iba vtedy, keď je úložisko ControlVault v systému prítomné.

Správa úložiska ControlVault

Tieto funkcie umožňujú správcovi systému spravovať systémové úložiská ControlVault.

Stav
Zobrazí pre úložisko ControlVault stav *aktívny* alebo *neaktívny*. Stav „Neaktívny“ znamená, že vo vašom systéme nie je možné do úložiska ControlVault ukladať. To, či váš systém Dell obsahuje úložisko ControlVault zistíte v jeho dokumentácii.

Heslo
Informuje o tom, či je nastavené heslo správcu ControlVault, a umožňuje heslo nastaviť nebo zmeniť (ak je už nastavené). Toto heslo môžu nastavovať a meniť iba správcovia systému. Heslo správcu ControlVault sa musí nastaviť tak, aby bolo možné vykonať tieto akcie:

- Archivácia a obnovenie údajov.
- Vymazanie používateľských údajov (pre všetkých používateľov).

POZNÁMKA: Ak sa používateľ pokúsi o archivovanie alebo obnovenie a zároveň nie je nastavené heslo správcu ControlVault, bude vyzvaný na jeho vytvorenie (ak ním nie je správca).

Zaregistrovaní používatelia
Informuje o používateľoch, ktorí zaregistrovali prihlasovacie údaje (napr. heslá, otlačky prstov či karty Smartcard) aktuálne uložené v úložisku ControlVault.

Vymazanie používateľských údajov
Údaje v úložisku ControlVault môže byť potrebné v niektorých prípadoch vymazať. Napríklad ak majú používatelia problémy s používaním alebo registrovaním údajov pre overenie pred spustením systému Windows. Všetky údaje uložené v úložisku ControlVault je možné pre jedného alebo všetkých používateľov vymazať pomocou tohto okna.

Na vymazanie všetkých používateľských údajov na platforme je potrebné zadať heslo správcu ControlVault. Ak sú zaregistrované údaje pre prihlásenie pred spustením systému Windows, budete vyzvaní tiež na zadanie systémového hesla. Po vymazaní všetkých používateľských údajov sa heslo správcu ControlVault a systémové heslo resetujú. To je jediný spôsob, ako vymazať heslo správcu ControlVault.

POZNÁMKA: Po vymazaní používateľských údajov budete vyzvaní na reštartovanie počítača. Reštart je dôležitý pre správnu funkciu systému.

Heslo správcu ControlVault nemusí byť nastavené kvôli vymazaniu údajov jedného používateľa. Po kliknutí na položku **vymazať používateľské údaje** budete vyzvaní na výber používateľa, ktorého údaje ControlVault chcete vymazať. Po výbere používateľa budete vyzvaní na zadanie systémového hesla (iba ak sú zaregistrované údaje pre prihlásenie pred spustením systému Windows).

POZNÁMKY:

- Ak pri vytváraní hesla správcu ControlVault nastane chyba, archivujte údaje, vymažte všetky používateľské údaje z úložiska ControlVault, reštartujte počítač a skúste vytvoriť heslo znovu.

- Ak pri vymazaní údajov z úložiska ControlVault pre jedného používateľa dôjde k chybe, archivujte svoje údaje, skúste vymazať všetky používateľské údaje a potom sa znovu pokúste vymazať údaje pre daného používateľa.
- Ak pri vymazaní údajov z úložiska ControlVault pre všetkých používateľov nastane chyba, zvážte reset systému. **Dôležité!** Pred resetovaním si prečítajte témy pomocníka Reset systému, pretože dôjde k vymazaniu VŠETKÝCH používateľských údajov zabezpečenia.
- Ak pri zálohovaní údajov ControlVault a TPM nastane chyba, deaktivujte modul TPM v systémeBIOS. To vykonáte reštartovaním počítača, vstupom do nastavenia systému BIOS stlačením klávesu **F2** počas spustenia a prechodom do časti Security>TPM Security. Potom znovu aktivujte modul TPM a znovu se pokúste o archiváciu údajov ControlVault.
- Podrobnejšie informácie o konkrétnych chybových správach nájdete na adrese wave.com/support/Dell.

Jednotky s automatickým šifrovaním: Rozšírené

Aplikácia **Dell Data Protection | Access** spravuje hardvérové bezpečnostné funkcie jednotiek s automatickým šifrovaním, ktoré majú šifrovanie údajov zabudované vo svojom hardvéri. Táto správa zabezpečuje, aby pri povolenom uzamknutí jednotky mali k šifrovaným údajom prístup iba autorizovaní používatelia.

Okno Jednotka s automatickým šifrovaním v časti **Správa zariadení** sa zobrazí iba v prípade, že sa v systéme nachádza jedna alebo viac jednotiek s automatickým šifrovaním (SED).

Dôležité! Po nastavení jednotky sú povolené funkcie ochrany údajov jednotky s automatickým šifrovaním a uzamykanie jednotky.

Správa zariadení

Tieto funkcie umožňujú správcovi jednotky spravovať nastavenia zabezpečenia jednotky. Zmeny vykonané na nastaveniach zabezpečenia jednotky sa prejavia po vypnutí jednotky.

Ochrana údajov

Zobrazuje stav *povolené* alebo *zakázané* pre ochranu údajov jednotky s automatickým šifrovaním. Stav „povolené“ znamená, že zabezpečenie jednotky je zapnuté. Pokiaľ však nie je aktivované *uzamykanie* jednotky, používatelia nemusia pred spustením systému Windows pri prístupe vykonať overenie pre jednotku.

Ochranu údajov jednotky s automatickým šifrovaním môžete deaktivovať tu. Ak je zakázané, všetky rozšírené funkcie zabezpečenia jednotky s automatickým šifrovaním sú vypnuté a jednotka sa správa ako štandardný disk. Deaktivácia ochrany údajov tiež vymaže všetky bezpečnostné nastavenia vrátanie údajov správcu jednotky a ich používateľov. Táto funkcia však nezmení ani neodstráni žiadne používateľské údaje v jednotke.

Uzamykanie

Zobrazuje stav *povolené* alebo *zakázané* pre jednotky s automatickým šifrovaním. Informácie o správaní uzamknutej jednotky nájdete v téme Jednotka s automatickým šifrovaním.

Môže byť nutné dočasne zakázať uzamykanie jednotky, čo môžete vykonať tu. Zakázanie uzamykania jednotky sa neodporúča, pretože v takom prípade sa pri prístupe k jednotke nevyžaduje žiadne overenie a k údajom má prístup akýkoľvek používateľ platformy. Pri zakázaní uzamykania jednotkysa zachovajú všetky nastavenia zabezpečenia vrátane údajov správcu a používateľov jednotky a všetkých používateľských údajov na jednotke.

POZOR! Ak chcete odinštalovať aplikáciu**Dell Data Protection | Access**, musíte najskôr zakázať ochranu údajov jednotky s automatickým šifrovaním a odomknúť jednotku.

Správca jednotky

Zobrazí aktuálneho správcu jednotky. Správca jednotky môže z tohto miesta určiť iného používateľa ako správcu jednotky. Nový správca musí byť v systéme platný používateľ systému Windows s oprávneniami správcu. V systému smie existovať iba jeden správca jednotky.

Používatelia jednotky

Zobrazí zaregistrovaných používateľov jednotky a počet aktuálne zaregistrovaných používateľov. Maximálny podporovaný počet používateľov závisí od jednotky s automatickým šifrovaním (aktuálne 4 používatelia v prípade jednotiek Seagate a 24 pri jednotkách Samsung).

Synchronizácia s heslom k systému Windows
Funkcia synchronizácie s heslom k systému Windows (WPS) automaticky nastaví heslá používateľov jednotky s automatickým šifrovaním tak, aby sa zhodovali s ich heslom k systému Windows. Táto funkcia sa nevynucuje v prípade správcu jednotky, vzťahuje se iba na používateľov jednotky. Funkciu WPS môžete použiť v podnikových prostrediach, kde sa heslá musia meniť v pravidelných intervaloch (napr. každých 90 dní). Pokiaľ je táto možnosť povolená, heslá k jednotke s automatickým šifrovaním všetkých používateľov sa pri zmene hesiel systému Windows automaticky zmenia.

POZNÁMKA: Ak je synchronizácia s heslom k systému Windows povolená (WPS), heslo používateľa jednotky s automatickým šifrovaním nie je možné zmeniť. Je potrebné zmeniť heslo k systému Windows a heslo k jednotke bude automaticky aktualizované.

Zapamätať posledné používateľské meno
Ak je tato možnosť povolená, posledné zadané používateľské meno bude v poli **Používateľské meno** obrazovky overenia pred spustením systému Windows zobrazené ako východzie.

Výber používateľského mena
Ak je táto možnosť povolená, používatelia môžu v poli **používateľské meno** obrazovky overenia pred spustením systému Windows prezerať mená všetkých používateľov jednotky.

Kryptografické vymazanie
Túto možnosť je možné použiť k „vymazaniu“ všetkých údajov na jednotke s automatickým šifrovaním. Nedôjde ku skutočnému odstráneniu údajov, ale k vymazaniu kľúčov používaných pre šifrovanie údajov, čo spôsobí nepoužiteľnosť údajov. Po kryptografickom vymazaní neexistuje žiadny spôsob, ako údaje obnoviť. Deaktivuje sa tiež ochrana údajov jednotky s automatickým šifrovaním a jednotka je pripravená k opätovnému použitiu.

POZNÁMKY:
- Pokiaľ dôjde k akýmkoľvek problémom týkajúcich sa funkcií správy jednotky s automatickým šifrovaním, úplne vypnite počítač (nereštartujte) a znovu ho spustite.
- Podrobnejšie informácie o konkrétnych chybových správach nájdete na adrese wave.com/support/Dell.

Informácie o overovacom zariadení

Okno Informácie o overovacom zariadení v časti **Správa zariadení** zobrazuje informácie a stav všetkých overovacích zariadení (tj. čítača otlačkov prstov, tradičné nebo bezkontaktné čítače kariet Smartcard) pripojených do systému.

Technická podpora

Technickú podporu softvéru **Dell Data Protection | Access** nájdete na adrese http://www.wave.com/support.dell.com.

CSP na báze TCG spoločnosti Wave

Poskytovateľ kryptografických služieb (CSP) s technológiou Wave Systems Trusted Computing Group (TCG) je súčasťou aplikácie **Dell Data Protection | Access** a je k dispozícii pre použitie vždy, keď sa vyžaduje poskytovateľ CSP – či už priamo volaný aplikáciou, alebo pripravený na výber zo zoznamu nainštalovaných poskytovateľov CSP. Vždy, keď je to možné, vyberajte možnosť „CSP na báze TCG spoločnosti Wave“, aby bolo zabezpečené vytvorenie kľúčov modulom TPM a že kľúče a ich heslá budú spravované aplikáciou **Dell Data Protection | Access**.

Technologie CSP funguje na báze TCG spoločnosti Wave Systems a umožňuje aplikáciám využívať funkcie dostupné na platformách v súlade s TCG priamo prostredníctvom MSCAPI. Ide o modul MSCAPI CSP podporovaný technológiou TCG, ktorý poskytuje asymetrickú funkčnosť kľúčov na module TPM a využíva zvýšenú bezpečnosť poskytovanú modulom TPM bez ohľadu na požiadavky špecifické pre dodávateľa týkajúcich sa poskytovateľa Trusted Software Stuck (TSS).

POZNÁMKA: Pokiaľ kľúče TPM vygenerované poskytovateľom CSP na báze TCG spoločnosti Wave vyžadujú heslo a používateľ vytvoril hlavné heslo TPM, heslá jednotlivých kľúčov sa náhodne vygenerujú a uložia v schránke hesiel TPM.