Domovská stránka Dell Data Protection | Access

Domovská stránka **Dell Data Protection | Access** je počátečním bodem přístupu k funkcím této aplikace. Z tohoto okna máte přístup k následujícím akcím:

Průvodce přístupem k systému
Možnosti přístupu
Jednotka s automatickým šifrováním
Rozšířené možnosti

V pravém dolním rohu okna je odkaz **Rozšířené** pomocí kterého lze zobrazit rozšířená nastavení.

Z okna rozšířené možnosti se můžete klepnutím na odkaz **domů** v pravém dolním rohu vrátit na domovskou stránku.

Průvodce přístupem k systému

Průvodce přístupem k systému se automaticky spustí při prvním spuštění aplikace **Dell Data Protection | Access**. Tento průvodce vás provede nastavením všech aspektů zabezpečení vašeho systému, včetně nastavení jak (např. pouze heslem nebo otiskem prstu a heslem) a kdy (před spuštěním systému Windows, při spuštění nebo obojí) má přihlášení k systému probíhat. Pokud má váš systém navíc jednotku s automatickým šifrováním, můžete ji nakonfigurovat prostřednictvím tohoto průvodce.

Funkce správce

Uživatelé, kteří mají oprávnění správce systému Windows, mají oprávnění používat v aplikaci **Dell Data Access | Protection** následující funkce, které standardní uživatlé používat nemohou:

- Nastavení / změna systémového hesla (před systémem Windows)
- Nastavení / změna hesla pevného disku
- Nastavení / změna hesla správce
- Nastavení / změna hesla vlastníka čipu TPM
- Nastavení / změna hesla správce ControlVault
- Reset systému
- Archivace a obnovení údajů
- Nastavení / změna kódu PIN správce karet Smartcard
- Vymazání / reset karty Smartcard
- Povolení / zakázání zabezpečeného přihlášení Dell k systému Windows
- Nastavení zásad přihlášení do systému Windows
- Správa jednotek s automatickým šifrováním:
    - Povolení / zakázání zamykání jednotky s automatickým šifrováním
    - Povolení / zakázání synchronizace hesla Windows (WPS)
    - Povolení / zakázání jednotného přihlášení (SSO)
    - Provedení kryptografického vymazání

Vzdálená správa

Vaše organizace si může vytvořit prostředí, ve kterém je možné centrálně spravovat bezpečnostní funkce aplikace **Dell Data Protection | Access** na více platformách (tj. vzdálená správa). V takovém případě lze použít bezpečnostní infrastrukturu systému Windows, například Active Directory, k bezpečné správě konkrétních funkcí aplikace **Dell Data Protection | Access**.

Když je počítač vzdáleně spravován (tj. „ve vlastnictví“ vzdáleného správce), místní správa funkcí aplikace **Dell Data Protection | Access** bude znemožněna a okna pro správu aplikace nebudou lokálně přístupná. Vzdáleně je možné spravovat následující funkce:

- Trusted Platform Module (TPM)
- ControlVault
- Přihlášení před spuštěním systému Windows
- Reset systému
- Hesla systému BIOS
- Zásady přihlašování do systému Windows
- Jednotky s automatickým šifrováním
- Registrace otisků prstů a karet Smartcard

Další informace o používání serveru EMBASSY® Remote Administration Server (ERAS) společnosti Wave Systems ke vzdálené správě získáte od svého prodejce společnosti Dell nebo na adrese dell.com.

Možnosti přístupu

V okně Možnosti přístupu můžete nastavovat způsob získávání přístupu do systému.

Pokud máte nastaveny možnosti aplikace **Dell Data Protection | Access**, budou zobrazeny na domovské stránce mezi dostupnými možnostmi (např. změnit heslo přihlášení před spuštěním systému Windows). Dostupné možnosti jsou zkratky, které vás po klepnutí přenesou do odpovídajícího okna k provedení konkrétního úkonu (např. změně hesla přihlášení před spuštěním systému Windows nebo registraci nového otisku prstu).

Obecné
Nejprve máte možnost určit, kdy má proběhnout přihlášení (před spuštěním systému Windows, po spuštění nebo obojí) a jak (např. otisk prstu a heslo). Můžete zvolit jednu nebo dvě možnosti způsobu připojení – například kombinace otisku prstu, karty Smartcard a hesla. Uvedené možnosti jsou založeny na zásadách přihlašování používaných ve vašem prostředí a na podpoře platformy.

Otisk prstu
Pokud systém obsahuje čtečku otisků prstů, můžete registrovat a aktualizovat otisky prstů pro použití k přihlášení do systému. Po zaregistrování otisků prstů můžete přejetím zaregistrovaného prstu přes čtečku otisků získat přístup do systému v přihlášení před nebo po spuštění systému Windows či v obou (v závislosti na nastavení obecných možností přístupu). Další informace najdete v části Registrace uživatelských otisků prstů.

Přihlášení před spuštěním systému Windows
Pokud jste rozhodli, že se uživatelé musí přihlašovat před spuštěním systému Windows, je třeba nastavit systémové heslo (jinak také heslo před spuštěním systému Windows) ke spuštění systému Windows. Jakmile je toto heslo nastaveno, správce jej může kdykoli měnit.

Na této obrazovce můžete přihlášení před spuštěním systému Windows také zakázat – je třeba zadat aktuální systémové heslo, potvrdit, že je heslo správné, a poté klepnout na tlačítko **Zakázat**.

Karta Smartcard
Pokud jste rozhodli, že uživatelé musí k přihlášení použít kartu Smartcard, je třeba zaregistrovat jednu nebo více tradičních (s kontakty) nebo bezkontaktních karet Smartcard. Klepnutím na odkaz **Zaregistrovat další kartu Smartcard** spustíte průvodce registrací karet Smartcard. Registrace znamená nastavení karty Smartcard pro použití k přihlášení.

Jakmile je karta Smartcard zaregistrována, můžete nastavit nebo změnit kód PIN této karty pomocí odkazu **Nastavit nebo změnit kód PIN karty Smartcard**.

Přihlášení před spuštěním systému Windows

Když je nastaveno přihlášení před spuštěním systému Windows, ověření (heslo, otisk prstu nebo karta Smartcard) je vyžadováno po spuštění systému ještě před tím, než se spustí systém Windows. Funkce přihlášení před spuštěním systému Windows poskytuje systému dodatečné zabezpečení tak, že brání neoprávněným uživatelům ve vstupu do systému Windows a přístupu k počítači (např. pokud byl odcizen).

V okně Přihlášení před spuštěním systému Windows mohou správci přihlášení nastavovat a vytvářet nebo měnit heslo před spuštěním systému Windows (systémové). Pokud je heslo již nastaveno, v tomto okně můžete přihlášení před spuštěním systému Windows deaktivovat. Nastavení přihlášení před spuštěním systému Windows spustí průvdoce s následujícími akcemi:

- Systémové heslo: Nastavení systémového hesla (heslo před spuštěním systému Windows) pro přístup před spuštěním systému Windows. Toto heslo je také používáno jako záloha v případě, kdy má uživatel dodatečné faktory ověřování (např. aby bylo možné získat přístup do systému v případě, že dojde k problému se čtečkou otisků prstů).
- Otisk prstu a karta Smartcard: Nastavte otisk prstu nebo kartu Smartcard pro použití k přihlášení před spuštěním systému Windows a určete, zda má být tento faktor ověřování používán jako náhrada hesla nebo jeho doplněk.
- Jednotné přihlášení: Standardně bude vaše ověření před spuštěním systému Windows (heslo, otisk prstu či karta Smartcard) použito také k automatickému přihlášení do systému Windows (to se nazývá „Jednotné přihlášení“). Tuto funkci zrušíte zaškrtnutím políčka „Zachovat přihlášení v systému Windows“.
- Pokud bylo kromě hesla před spuštěním systému Windows nastaveno také heslo pevného disku systému BIOS, máte také možnost změnit nebo zrušit heslo pevného disku.

POZNÁMKA: Ne všechny čtečky otisků prstů lze použít k ověření před spuštěním systému Windows. Pokud vaše čtečka není kompatibilní, můžete registrovat otisky prstů pouze pro přihlášení v systému Windows. Informace o kompatibilních čtečkách otisků prstů získáte od správce systému a na adrese support.dell.com najdete seznam podporovaných čteček otisků.

Deaktivace přihlášení před spuštěním systému Windows
V tomto okně můžete přihlášení před spuštěním systému Windows také zakázat – je třeba zadat aktuální heslo před spuštěním systému Windows (systémové), potvrdit, že je heslo správné, a poté klepnout na tlačítko **Zakázat**. Když zakážete přihlášení před spuštěním systému Windows, zaregistrované otisky prstů a karty Smartcard zůstanou zaregistrované.

Registrace otisků prstů

Uživatelé mohou registrovat nebo aktualizovat otisky prstů pro použití k ověření systémem při nebo před spuštěním systému Window. Na kartě Otisk prstu obrázky rukou znázorňují, které prsty byly zaregistrovány. Po klepnutí na odkaz **Zaregistrovat další** se spustí průvodce registrací otisků prstů, který vás provede procesem registrace. „Registrace“ znamená uložení otisku prstu pro použití k přihlášení. Aby byla registrace možná, musí být správně nainstalována a nakonfigurována platná čtečka otisků prstů.

POZNÁMKA: Ne všechny čtečky otisků prstů lze použít k přihlášení před spuštěním systému Windows. Pokud se s nekompatibilní čtečkou pokusíte zaregistrovat otisky k přihlášení před spuštěním systému Windows, zobrazí se chybová zpráva. Informace o kompatibilních zařízeních získáte od správce systému a na adrese support.dell.com najdete seznam podporovaných čteček otisků.

Při registraci otisku prstu budete vyzváni k ověření vaší identity zadáním hesla systému Windows. Pokud to vaše zásady vyžadují, budete vyzváni také k zadání hesla před spuštěním systému Windows (systémového). Heslo před spuštěním systému Windows lze použít k získání přístupu do systému v případě, že dojde k problému se čtečkou otisků prstů.

POZNÁMKY:

- Doporučuje se během procesu registrace zaregistrovat alespoň dva otisky prstů.
- Před aktivací ověření pomocí otisků prstů je třeba zajistit, aby byly otisky prstů řádně zaregistrovány.
- Pokud v systému vyměníte čtečku otisků, je třeba otisky prstů znovu zaregistrovat s novou čtečkou. Přepínání mezi dvěma různými čtečkami otisků prstů se nedoporučuje.
- Pokud se vám při registraci otisků prstů opakovaně zobrazuje zpráva „snímač ztratil zaostření“, je možné, že počítač čtečku otisků prstů nerozpoznává. Pokud je čtečka otisků externí, její odpojení a opětovné připojení problém v mnoha případech odstraní.

Vymazání registrovaných otisků prstů

Zaregistrované otisky prstů můžete odebírat klepnutím na odkaz **Odebrat otisk prstu** nebo klepnutím na zaregistrovaný prst (zrušením vybrání) v průvodci registrací otisků prstů.

Konkrétního uživatele s otisky prstů zaregistrovanými pro ověření před spuštěním systému Windows může správce odebrat zrušením výběru všech otisků prstů zaregistrovaných uživatelem.

POZNÁMKA: Pokud během procesu registrace otisků prstů dojde k chybám, další podrobnosti najdete na adrese wave.com/support/Dell.

Registrace karet Smartcard

Dell Data Protection | Access umožňuje používat tradiční (s kontakty) nebo bezkontaktní karty Smartcard pro přihlašování k účtu systému Windows nebo k ověření před spuštěním systému Windows. Na kartě Smartcard klepnutím na odkaz **Zaregistrovat další kartu Smartcard** spusťte průvodce registrací karty Smartcard, který vás provede procesem registrace. „Registrace“ znamená nastavení karty Smartcard pro použití k přihlášení.

Aby byla registrace možná, musí být správně nainstalováno a nakonfigurováno platné zařízení k ověřování karet Smartcard.

POZNÁMKA: Informace o kompatibilních zařízeních získáte od správce systému a na adrese support.dell.com najdete seznam podporovaných karet Smartcard.

Registrace
Při registraci karty Smartcard budete vyzváni k ověření vaší identity zadáním hesla systému Windows. Pokud to vaše zásady vyžadují, budete vyzváni také k zadání hesla před spuštěním systému Windows (systémového). Heslo před spuštěním systému Windows lze použít k získání přístupu do systému v případě, že dojde k problému se čtečkou karet Smartcard.

Během registrace budete vyzváni k zadání kódu PIN karty Smartcard, pokud byl nastaven. Pokud vaše zásady vyžadují kód PIN a žádný nebyl nastaven, budete vyzváni k jeho vytvoření.

POZNÁMKY:

- Jakmile je uživatel zaregistrován pro použití karty Smartcard k přihlášení před spuštěním systému Windows, nelze uživatele odebrat.
- Standardní uživatelé mohou měnit uživatelský kód PIN karty Smartcard a správce může měnit jak správcovský tak uživatelský kód PIN.
- Správce může také resetovat kartu Smartcard. Po resetování kartu Smartcard nelze použít k ověření při nebo před spuštěním systému Windows, dokud nebude znovu zaregistrována.

POZNÁMKA:V případě ověřování certifikátů TPM mohou správci registrovat certifikáty TPM prostřednictvím procesu registrace karet Smartcard systému Microsoft Windows. Aby byla zajištěna kompatibilita s touto aplikací, správce musí jako poskytovatele kryptografických služeb zvolit možnost „CSP na bázi TCG společnosti Wave“ namísto CSP karty Smartcard. Navíc musí být povolena funkce zabezpečeného přihlášení Dell s odpovídající zásadou typu ověření pro klienta.

POZNÁMKA: Pokud se zobrazí chybová zpráva, že služba Smartcard není spuštěna, můžete ji spustit/restartovat následovně:

- Přejděte z Ovládacích panelů do okna Nástroje správy, vyberte položku Služba, klepněte pravým tlačítkem na položku Smartcard a vyberte možnost Spustit nebo Restartovat.
- Podrobnější informace o konkrétních chybových zprávách najdete na adrese wave.com/support/Dell.

Jednotka s automatickým šifrováním

Aplikace **Dell Data Protection | Access** spravuje hardwarové bezpečnostní funkce jednotek s automatickým šifrováním, které mají šifrování dat vestavěno ve svém hardwaru. Tato funkce zajišťuje, aby měli k šifrovaným datům přístup pouze autorizovaní uživatelé (když je povoleno uzamykání jednotky).

Okno Jednotka s automatickým šifrováním otevřete klepnutím na spodní kartu **Jednotka s automatickým šifrováním**. Tato karta se zobrazuje pouze v případě, že je v systému přítomna jedna nebo více jednotek s automatickým šifrováním (SED).

Klepnutím na odkaz **Nastavení** spustíte průvodce nastavením jednotky s automatickým šifrováním. V tomto průvodci můžete vytvořit heslo správce jednotky, toto heslo zálohovat a použít nastavení šifrování jednotky. K průvodci nastavením jednotky s automatickým šifrováním mají přístup pouze správci systému.

Důležité! Po nastavení jednotky jsou „povoleny“ funkce ochrany dat a uzamykání jednotky. Když je jednotka uzamknuta, platí následující chování:

- Jednotka přejde do režimu *zamknuto* kdykoli je vypnuto její napájení.
- Jednotka se nespustí, pokud uživatel nezadá správné uživatelské jméno a heslo (nebo otisk prstu) na obrazovce přihlášení před spuštěním systému Windows. Dokud není povoleno uzamykání jednotky, data v ní jsou přístupná všem uživatelům počítače.
- Jednotka je zabezpečena i v případě, že je připojena jako sekundární jednotka k jinému počítači – při pokusu o přístup k datům v jednotce je vyžadováno ověření.

Jakmile je jednotka nastavena, okno Jednotka s automatickým šifrováním zobrazí jednotky a odkaz pro uživatele ke změně jejich hesel k jednotkám. Pokud jste správce jednotky, můžete v tomto okně také přidávat a odebírat uživatele jednotek. Pokud je přítomna externí jednotka a byla nastavena, zobrazí se v tomto okně a je možné ji odemknout.

POZNÁMKA: Aby bylo možné uzamknout sekundární externí jednotku, musí být vypnuta nezávisle na počítači.

Správce jednotky může spravovat nastavení jednotky v části **Rozšířené>Zařízení**. Další informace najdete v části Správa zařízení – Jednotky s automatickým šifrováním.

Nastavení jednotky

Průvodce nastavením jednotky s automatickým šifrováním vás provede nastavením jednotek. Během tohoto procesu je důležité mít na paměti následující koncepty.

Správce jednotky
První uživatel s oprávněními správce systému, který nastaví přístup k jednotce (a nastaví heslo správce jednotky), se stane správcem jednotky. Tento uživatel má jako jediný oprávnění provádět změny přístupu k jednotce. Abyste potvrdili, že první uživatel je úmyslně nastavován jako správce jednotky, a bylo možné pokračovat k dalšímu kroku, je třeba zaškrtnout políčko „Rozumím“.

Heslo správce jednotky
Průvodce vás vyzve k vytvoření hesla správce jednotky a k opětovnému zadání tohoto hesla pro potvrzení. Než budete moci vytvořit heslo správce jednotky, musíte prokázat svoji identitu zadáním hesla k systému Windows. Aby mohl vytvořit toto heslo, musí mít aktuální uživatel systému Windows oprávnění správce.

Zálohování přihlašovacích údajů jednotky
Zadáním nebo klepnutím na tlačítko **Procházet** zvolte umístění, do kterého chcete uložit záložní kopii vašich údajů správce jednotky.

DŮLEŽITÉ**!**

- Tyto přihlašovací údaje je silně doporučováno zálohovat a to jinam než na primární pevný disk (např. na vyměnitelné médium). Jinak byste v případě ztráty přístupu k jednotce nebyli schopni přistupovat ani k záloze.
- Po dokončení nastavení jednotky budou při příštím spuštění systému všichniuživatelé muset před spuštěním systému Windows zadat správné uživatelské jméno a heslo (nebo otisk prstu).

Přidání uživatele jednotky
Správce jednotky může k jednotce přidávat další platné uživatele systému Windows. Při přidání uživatele k jednotce má správce možnost vyžadovat od uživatele resetování jeho hesla při prvním přihlášení. Od uživatele bude před odemknutím jednotky vyžadováno resetovat své heslo na obrazovce ověření před spuštěním systému Windows.

Rozšířená nastavení

- *Jednotné přihlášení* – Standardně bude vaše heslo k jednotce s automatickým šifrováním, které zadáváte jako ovření pro jednotku před spuštěním systému Windows, použito také k automatickému přihlášení do systému Windows (tato funkce se nazývá „Jednotné přihlášení“). Tuto funkci můžete deaktivovat políčkem „Chci se znovu přihlásit při spuštění systému Windows“ při konfiguraci nastavení jednotky.
- *Přihlášení otiskem prstu* – Na podporovaných platformách můžete určit, že chcete k ověření pro jednotku s automatickým šifrováním používat otisk prstu místo hesla.
- *Podpora režimu spánku/pohotovostního režimu (S3)* (pokud je na platformě podporován) – Pokud je tato funkce aktivní, vaši jednotku s automatickým šifrováním lze bezpečně uvést do režimu spánku/pohotovostního režimu (jinak také režimu S3) a při obnovení z režimu spánku/pohotovostního režimu bude vyžadováno ověření před spuštěním systému Windows.

POZNÁMKY:

- Když je aktivní podpora režimu S3, hesla šifrování jednotky podléhají jakýmkoli existujícím nárokům na hesla systému BIOS. Další informace o jakýchkoli konkrétních existujících omezeních pro hesla systému BIOS získáte od výrobce hardwaru systému.
- Ne všechny jednotky s automatickým šifrováním podporují režim S3. Během nastavení jednotky budete informováni o tom, zda jednotka režim spánku/pohotovostní režim podporuje či nikoli. V případě jednotek, které tento režim nepodporují, budou požadavky typu S3 systému Windows automaticky převáděny na požadavky k hibernaci, pokud je režim hibernace povolen (je silně doporučováno, aby režim hibernace byl v počítači povolen).
- Při prvním přihlášení po aktivaci možnosti jednotného přihlášení (SSO) se proces při výzvě k přihlášení do systému Windows zastaví. Budete vyzváni k přihlášení do systému Windows vámi zvoleným způsobem, který bude bezpečně uložen pro účely budoucího přihlašování k systému Windows. Při dalším spuštění systému vás funkce SSO automaticky přihlásí k systému Windows. Stejný proces je vyžadován také tehdy, když se změní ověření uživatele pro systém Windows (heslo, otisk prstu, kód PIN karty Smartcard). Pokud se počítač nachází na doméně, která má zásadu vyžadující stisknutí kláves ctrl+alt+del před spuštěním systému Windows, tato zásada bude respektována.

POZOR!Pokud chcete odinstalovat aplikaci **Dell Data Protection | Access**, musíte nejprve zakázat ochranu dat jednotky s automatickým šifrováním a odemknout jednotku.

Uživatelské funkce SED

Správci jednotek s automatickým šifrováním obstarávají veškerou správu zabezpečení jednotky a uživatelů. Uživatelé jednotky, kteří nejsou jejími správci, mohou provádět pouze následující úkony:

- Měnit své vlastní heslo k jednotce
- Odemknout jednotku

Tyto úkony lze provádět z karty **Jednotka s automatickým šifrováním** v aplikaci **Dell Data Protection | Access**.

Změna hesla
Umožňuje zaregistrovaným uživatelům vytvořit nové ověřovací heslo jednotky. Před nastavením hesla jednotky s automatickým šifrováním na novou hodnotu je třeba zadat aktuální heslo jednotky.

POZNÁMKY:

- Aplikace bude vynucovat dodržení zásad systému Windows pro délku a složitost hesla, pokud jsou nastaveny. Pokud nejsou zásady systému Windows pro vytváření hesel nastaveny, maximální délka hesla jednotky s automatickým šifrováním je 32 znaků. V případě, že není povolen režim S3 (režim spánku/pohotovostní režim), maximální délka je 127 znaků.
- Heslo uživatele k jednotce s automatickým šifrováním není shodné s heslem do systému Windows. Pokud se uživatelské heslo k systému Windows změní nebo resetuje, nemá to vliv na uživatelské heslo jednotky v případě, že nebyla aktivována synchronizace s heslem k systému Windows. Podrobnosti najdete v části Zařízení: Jednotky s automatickým šifrováním.
- Na některých klávesnicích v jiném než anglickém jazyce existují znaky, které nelze v hesle jednotky s automatickým šifrováním použít. Pokud heslo systému Windows obsahuje některý z níže uvedených znaků a je povolena synchronizace s heslem k systému Windows, synchronizace se nezdaří a zobrazí se chybová zpráva.

Odemknutí jednotky
Odemknutí jednotky umožňuje zaregistrovanému uživateli odemknout uzamknutou jednotku. Pokud je povoleno uzamykání jednotky, jednotka přejde do uzamčeného stavu kdykoli, když je vypnuto napájení počítače. Při příštím spuštění systému je třeba provést ověření pro jednotku zadáním hesla na obrazovce přihlášení před spuštěním systému Windows.

POZNÁMKY:

- Pokud je na počítači současně aktivních více účtů uživatelů jednotky s automatickým šifrováním, může být nemožné vstoupit do úsporného režimu (tj. režimu spánku/pohotovostního režimu nebo hibernace).
- Na ověřovací obrazovce před spuštěním systému Windows jsou jména uživatelů jednotky nahrazena názvy „User 1“, „User 2“ atd. ve verzích aplikace lokalizovaných do těchto jazyků: čínština, japonština, korejština a ruština.

Rozšířené možnosti

Rozšířené možnosti aplikace **Dell Data Protection | Access** umožňují uživateli s oprávněními správce ovládat následující aspekty aplikace:

Údržba
Hesla
Zařízení

POZNÁMKA: Úpravy rozšířených možností mohou provádět pouze uživatelé s oprávněními správce; standardní uživatelé mohou tato nastavení prohlížet, ale nemohou provádět změny.

Údržba

Okno Údržba slouží správcům k nastavení předvoleb přihlašování k systému Windows, obnovení systému v přípravě na změnu použití nebo k archivaci či obnovení uživatelských údajů uložených v bezpečnostním hardwaru systému. Podrobnosti naleznete v následujících tématech:

Předvolby přístupu
Reset systému
Archivace a obnovení údajů

Předvolby přístupu

Okno Předvolby přístupu umožňuje správcům nastavovat předvolby přihlášení do systému Windows pro všechny uživatele systému.

Aktivace zabezpečeného přihlášení Dell
Možnost nahradit standardní obrazovku ctrl-alt-delete systému Windows umožňuje použít různé faktory ověřování namísto (nebo k posílení) hesla systému Windows pro přístup do systému Windows. Abyste posílili zabezpečení přihlášení k systému Windows, můžete jako druhý faktor ověřování přidat otisk prstu. Lze přidat také další faktory ověřování při přihlašování k systému Windows, včetně karty Smartcard nebo certifikátu TPM.

POZNÁMKY:

- Povolení zabezpečeného přihlášení Dell má vliv na všechny uživatele systému.
- Tuto možnost doporučujeme aktivovat AŽ POTÉ, co uživatelé zaregistrovali své otisky prstů nebo karty Smartcard.
- Při prvním přihlášení po nastavení této možnosti budete vyzváni k ověření pro systém Windows podle vašich standardních zásad a při dalším spuštění bude třeba použít nové faktory ověřování.

Deaktivace zabezpečeného přihlášení Dell
Tato možnost zakáže všechny funkce aplikace **Dell Data Protection | Access** k přihlašování do systému Windows. Pokud zvolíte tuto možnost, vrátíte se k používání standardních zásad přihlašování systému Windows.

POZNÁMKY:

- Pokud během přihlašování dojde k chybě týkající se zabezpečeného přihlášení Windows, deaktivujte a znovu aktivujte možnost zabezpečeného přihlášení Dell.
- Podrobnější informace o konkrétních chybových zprávách najdete na adrese wave.com/support/Dell.

Reset systému

Funkce Reset systému slouží k vymazání veškerých uživatelských dat z veškerého bezpečnostního hardwaru na platformě. Hodí se například při změně použití počítače. Tato možnost vymaže veškerá hesla systému kromě uživatelských hesel systému Windows a také veškerá data v hardwarových zařízeních (tj. úložiště ControlVault, modul TPM a čtečky otisků prstů). V případě jednotek s automatickým šifrováním tato funkce také zruší ochranu dat, takže jsou data na jednotce přístupná.

Musíte potvrdit, že si uvědomujete, že resetujete systém, a poté klepnout na tlačítko **Další**. Abyste mohli systém resetovat, musíte zadat heslo ke každému bezpečnostnímu zařízení, u kterého je nastaveno:

- Heslo vlastníka TPM
- Heslo správce ControlVault
- Heslo správce systému BIOS
- Heslo systému BIOS (před spuštěním systému Windows)
- Heslo pevného disku (BIOS)
- Heslo správce jednotky s automatickým šifrováním

POZNÁMKA: V případě jednotek s automatickým šifrováním je vyžadováno pouze heslo správce jednotky, ne hesla všech uživatelů jednotky.

Důležité! Jediným způsobem, jak lze data po resetu získat zpět, je jejich obnovením z dříve uloženého archivu. Pokud jste žádný archiv nevytvořili, data jsou ztracena. V případě jednotek s automatickým šifrováním jsou vymazána pouze data nastavení, osobní data na jednotce jsou zachována.

Archivace a obnovení údajů

Funkce Archivace a obnovení údajů slouží k zálohování a obnovení všech uživatelských údajů (přihlašovacích a šifrovacích údajů) uložených v úložišti ControlVault a na čipu TPM (Trusted Platform Module). Zálohování těchto dat je důležité při přerozdělování počítačů nebo k obnovení dat v případě selhání hardwaru. V takovém případě můžete jednoduše obnovit veškeré vaše údaje do nového počítače z uloženého souboru archivu.

Můžete archivovat a obnovovat údaje jednotlivých uživatelů nebo všech uživatelů v systému.

Uživatelské údaje obsahují data používaná k přihlášení před spuštěním systému Windows jako registrované otisky prstů a data karet Smartcard a klíče uložené v modulu TPM. Modul TPM vytváří klíče dle potřeby aplikací pro zabezpečení – například vytvoření digitálního certifikátu vytvoří klíče v modulu TPM.

POZNÁMKA: Informace o tom, zda lze klíče TPM archivovat pomocí aplikace Dell Data Protection | Access, najdete v dokumentaci zabezpečené aplikace. Souhrnně jsou podporovány aplikace, které ke generování klíčů používají „CSP na bázi TCG společnosti Wave“.

Archivace údajů
Archivace údajů se provádí následovně:

- Určete, zda chcete archivovat údaje pro sebe nebo pro všechny uživatele v systému.
- Poskytněte ověření zabezpečovacímu hardwaru zadáním systémového hesla (před spuštěním systému Windows), heslo správce ControlVault a heslo vlastníka modulu TPM.
- Vytvořte heslo zálohy údajů.
- Určete umístění archivu pomocí tlačítka **Procházet**. Umístěním archivu by mělo být vyměnitelné médium, jako je např. jednotka USB flash nebo síťová jednotka, aby byla záloha chráněna pro případ selhání pevného disku.

Důležité poznámky:
- Poznamenejte si umístění archivu, protože uživatel jej bude potřebovat znát k obnovení údajů.
- Poznamenejte si heslo zálohy údajů, aby bylo možné data obnovit. Tento krok je obzvláště důležitý, jelikož heslo nelze zpětně zjistit.
- Pokud neznáte heslo vlastníka modulu TPM, kontaktujte správce systému nebo nahlédněte do pokynů k nastavení modulu TPM počítače.

Obnovení údajů
Obnovení údajů se provádí následovně:

- Určete, zda chcete obnovit údaje pro sebe nebo pro všechny uživatele v systému.
- Vyhledejte umístění archivu a vyberte soubor archivu.
- Zadejte heslo zálohy údajů, které jste zadali při vytváření archivu.
- Poskytněte ověření zabezpečovacímu hardwaru zadáním systémového hesla (před spuštěním systému Windows), heslo správce ControlVault a heslo vlastníka modulu TPM.

POZNÁMKY:
- Pokud během obnovování údajů dojde k chybě a obnovení se nezdaří ani při dalších pokusech, zkuste provést obnovení z jiného souboru archivu. Pokud neuspějete, vytvořte jiný archiv údajů a pokuste se o obnovení z něj.
- Pokud dojde k chybě během obnovování klíčů TPM, vytvořte archiv údajů a poté vymažte modul TPM v systému BIOS. Chcete-li vymazat modul TPM, restartujte počítač, stisknutím klávesy **F2** během spouštění vstupte do nastavení systému BIOS a poté přejděte do části

Security>TPM Security. Zde obnovte vlastnictví modulu TPM a pokuste se o obnovení údajů znovu.

- Podrobnější informace o konkrétních chybových zprávách najdete na adrese wave.com/support/Dell.

Správa hesel

Z okna Správa hesel může správce vytvářet a měnit veškerá bezpečnostní hesla v systému:

- Systémové heslo (před spuštěním systému Windows)*
- Heslo správce*
- Heslo pevného disku*
- Heslo ControlVault
- Heslo vlastníka TPM
- Hlavní heslo TPM
- Heslo schránky hesel TPM
- Heslo jednotky s automatickým šifrováním

POZNÁMKY:

- Zobrazena budou pouze hesla platná pro aktuální konfiguraci platformy – toto okno se tedy mění v závislosti na konfiguraci a stavu systému.
- Hesla se symbolem * jsou hesla systému BIOS a lze je změnit také prostřednictvím systému BIOS.
- Hesla na úrovni systému BIOS nelze vytvářet ani měnit, pokud správce systému BIOS změny hesel zakázal.
- Klepnutím na odkaz **nastavení** u jednotky s automatickým šifrováním spustíte průvodce jejím nastavením. Po klepnutí na položku **spravovat** může uživatel změnit heslo jedné nebo více jednotek s automatickým šifrováním.
- Klepnutím na odkaz **spravovat** u Schránky hesel TPM zobrazíte okno, ve kterém můžete prohlížet a měnit hesla chránící vaše klíče TPM. Když je vytvořen klíč TPM, který vyžaduje vytvoření hesla, heslo je náhodně vygenerováno a umístěno do schránky. Schránku hesel TPM nemůžete spravovat, dokud nevytvoříte hlavní heslo TPM.

Pravidla komplexnosti hesel systému Windows

Aplikace **Dell Data Protection | Access** zajišťuje, aby následující hesla odpovídala pravidlům komplexnosti hesel počítače:

- Heslo vlastníka TPM

Chcete-li se seznámit s požadavky komplexnosti hesel daného počítače, postupujte podle následujících kroků:

1. Otevřete Ovládací panely.
2. Poklepejte na položku Nástroje správy.
3. Poklepejte na položku Místní zásady zabezpečení.
4. Rozevřete nabídku Zásady účtu a vyberte Zásady hesel.

Zařízení

Okno Zařízení slouží správcům ke správě všech bezpečnostních zařízení instalovaných v systému. U každého zařízení můžete prohlížet stav a další podrobné informace, jako je například verze firmwaru. Klepnutím na položku **ukázat** zobrazíte informace o jednotlivých zařízeních, nebo danou sekci můžete sbalit položkou **skrýt**. Ke spravovatelným zařízením patří následující v závislosti na tom, která z nich vaše platforma obsahuje:

Trusted Platform Module (TPM)
ControlVault®
Jednotky s automatickým šifrováním
Informace o ověřovacím zařízení

Trusted Platform Module (TPM)

Bezpečnostní čip TPM musí být povolen a jeho vlastnictví musí být určeno, aby bylo možné používat pokročilé funkce zabezpečení poskytované aplikací **Dell Data Protection | Access** a modulem TPM.

Okno Trusted Platform Module v sekci **Správa zařízení** se zobrazí pouze, když je modul TPM v systému přítomen.

Správa modulu TPM

Tyto funkce umožňují správci systému spravovat modul TPM.

Stav
Zobrazí pro modul TPM stav *aktivní* nebo *neaktivní*. Stav „Aktivní“ značí, že modul TPM je povolen v systému BIOS a je připraven k nastavení (tj. lze přijmout vlastnictví). Modul TPM nelze spravovat a jeho funkce zabezpečení nelze používat, pokud není aktivní (povolen).

Pokud je modul TPM v systému zjištěn ale není aktivní (povolen), můžete jej povolit klepnutím na odkaz **aktivovat** v tomto okně, aniž byste museli vstupovat do systému BIOS. Poté, co modul TPM pomocí této funkce povolíte, musí být počítač restartován. Během restartování se může zobrazit dotaz, který vás vyzve k potvrzení změn.

POZNÁMKA: Možnost povolení (aktivace) modulu TPM z této aplikace nemusí být podporována na všech platformách. Pokud podporována není, je třeba modul povolit v systému BIOS. To provedete restartováním systému, vstupem do nastavení systému BIOS stisknutím klávesy **F2** před načtením systému Windows, přechodem do části Security>TPM Security a aktivováním modulu TPM.

Na tomto místě můžete modul TPM také *deaktivovat* klepnutím na odkaz **deaktivovat**. Deaktivací modulu TPM způsobíte znepřístupnění pokročilých funkcí zabezpečení. Deaktivace však nezmění žádná nastavení modulu TPM a nevymaže ani nezmění žádné údaje ani klíče v modulu uložené.

Má vlastníka
Zobrazuje stav vlastnictví (tj. „má vlastníka“) a umožňuje určovat nebo měnit vlastníka modulu TPM. Vlastnictví modulu TPM musí být určeno, aby bylo možné využívat jeho funkce zabezpečení. Aby bylo možné určit vlastnictví, modul TPM musí být nejprve povolen (aktivován).

Proces určení vlastnictví znamená, že uživatel (s oprávněními správce) vytvoří Heslo vlastníka TPM. Jakmile je heslo definováno, je určeno vlastnictví a modul TPM je připraven k použití.

POZNÁMKA: Heslo vlastníka TPM musí odpovídat pravidlům komplexnosti hesel systému Windows ve vašem systému.

Důležité! Je důležité, abyste heslo vlastníka TPM neztratili nebo nezapomněli, jelikož je vyžadováno pro přístup k pokročilým funkcím zabezpečení modulu TPM v aplikaci **Dell Data Protection | Access**.

Uzamknuto
Zobrazí pro modul TPM stav *uzamknuto* nebo *odemknuto*. „Uzamykání“ je funkce zabezpečení modulu TPM. Modul TPM přejde do stavu uzamknutí po předem určeném počtu zadání nesprávného hesla vlastníka TPM. Vlastník modulu TPM jej může zde odemknout. Je vyžadováno zadání hesla vlastníka TPM.

POZNÁMKY:

- Pokud dojde k chybě při vytváření vlastnictví modulu TPM, vymažte modul TPM v systému BIOS a pokuste se o vytvoření vlastnictví znovu. Chcete-li vymazat modul TPM, restartujte počítač, stisknutím klávesy **F2** během spouštění vstupte do nastavení systému BIOS a poté přejděte do části Security>TPM Security.
- Pokud dojde k chybě při změně hesla vlastníka TPM, proveďte archivaci dat modulu TPM (archiv údajů), vymažte modul v systému BIOS, obnovte jeho vlastnictví a obnovte data modulu TPM (obnovení údajů).
- Podrobnější informace o konkrétních chybových zprávách najdete na adrese wave.com/support/Dell.

Dell ControlVault®

Dell ControlVault® (CV) je bezpečné hardwarové úložiště pro uživatelské údaje používané při přihlašování před spuštěním systému Windows (např. uživatelská hesla a zaregistrované otisky prstů). Okno ControlVault v sekci **Správa zařízení** se zobrazí pouze, když je úložiště ControlVault v systému přítomno.

Správa úložiště ControlVault

Tyto funkce umožňují správci systému spravovat systémové úložiště ControlVault.

Stav

Zobrazí pro úložiště ControlVault stav *aktivní* nebo *neaktivní*. Stav „Neaktivní“ značí, že ve vašem systému není možné do úložiště ControlVault ukládat. Zda váš systém Dell obsahuje úložiště ControlVault zjistíte v jeho dokumentaci.

Heslo

Informuje o tom, zda je nastaveno heslo správce ControlVault, a umožňuje heslo nastavit nebo změnit (pokud je již nastaveno). Toto heslo mohou nastavovat a měnit pouze správci systému. Heslo správce ControlVault musí být nastaveno, aby bylo možné provádět následující akce:

- Provedení archivace a obnovení údajů.
- Vymazání uživatelských dat (pro všechny uživatele).

POZNÁMKA: Pokud se uživatel pokusí o archivaci nebo obnovení, když není nastaveno heslo správce ControlVault, bude vyzván k jeho vytvoření (pokud se jedná o správce).

Zaregistrovaní uživatelé

Informuje o uživatelích, kteří zaregistrovali přihlašovací údaje (např. hesla, otisky prstů či karty Smartcard) aktuálně uložené v úložišti ControlVault.

Vymazání uživatelských dat

Data v úložišti ControlVault může být v některých případech nutné vymazat. Například pokud mají uživatelé problémy s používáním nebo registrováním údajů pro ověření před spuštěním systému Windows. Veškerá data uložená v úložišti ControlVault lze pro jednoho nebo všechny uživatele vymazat prostřednictvím tohoto okna.

K vymazání veškerých uživatelských dat na platformě je třeba zadat heslo správce ControlVault. Pokud jsou zaregistrovány údaje pro přihlášení před spuštěním systému Windows, budete vyzváni také k zadání systémového hesla. Po vymazání všech uživatelských dat jsou heslo správce ControlVault a systémové heslo resetovány. Toto je jediný způsob, jak vymazat heslo správce ControlVault.

POZNÁMKA: Po vymazání uživatelských dat budete vyzváni k restartování počítače. Restart je důležitý pro správnou funkci systému.

Heslo správce ControlVault nemusí být nastaveno kvůli vymazání údajů jednoho uživatele. Po klepnutí na položku **vymazat uživatelská data** budete vyzváni k výběru uživatele, jehož údaje ControlVault si přejete vymazat. Po výběru uživatele budete vyzváni k zadání systémového hesla (pouze pokud jsou zaregistrovány údaje pro přihlášení před spuštěním systému Windows).

POZNÁMKY:

- Pokud dojde k chybě při vytváření hesla správce ControlVault, proveďte archivaci údajů, vymažte veškerá uživatelská data z úložiště ControlVault, restartujte počítač a pokuste se vytvořit heslo znovu.

- Pokud dojde k chybě při vymazání údajů z úložiště ControlVault pro jednoho uživatele, archivujte své údaje, zkuste vymazat všechna uživatelská data a poté se znovu pokuste vymazat data pro daného uživatele.
- Pokud dojde k chybě při vymazání údajů z úložiště ControlVault pro všechny uživatele, zvažte provedení resetu systému. **Důležité!** Před provedením resetu si projděte téma nápovědy Reset systému, protože dojde k vymazání VŠECH uživatelských dat zabezpečení.
- Pokud dojde k chybě při zálohování dat ControlVault a TPM, deaktivujte modul TPM v systému BIOS. To provedete restartováním počítače, vstupem do nastavení systému BIOS stisknutím klávesy **F2** během spouštění a přechodem do části Security>TPM Security. Poté znovu aktivujte modul TPM a znovu se pokuste o archivaci dat ControlVault.
- Podrobnější informace o konkrétních chybových zprávách najdete na adrese wave.com/support/Dell.

Jednotky s automatickým šifrováním: Rozšířené

Aplikace **Dell Data Protection | Access**spravuje hardwarové bezpečnostní funkce jednotek s automatickým šifrováním, které mají šifrování dat vestavěno ve svém hardwaru. Tato správa zajišťuje, aby měli při povoleném uzamčení jednotky k šifrovaným datům přístup pouze autorizovaní uživatelé.

Okno Jednotka s automatickým šifrováním v části **Správa zařízení** se zobrazí pouze v případě, že je v systému přítomna jedna nebo více jednotek s automatickým šifrováním (SED).

Důležité! Po nastavení jednotky jsou povoleny funkce ochrany dat jednotky s automatickým šifrováním a uzamykání jednotky.

Správa zařízení
Tyto funkce umožňují správci jednotky spravovat nastavení zabezpečení jednotky. Změny provedené na nastaveních zabezpečení jednotky se projeví po vypnutí jednotky.

Ochrana dat
Zobrazuje stav *povoleno* nebo *zakázáno* pro ochranu dat jednotky s automatickým šifrováním. Stav „povoleno“ značí, že zabezpečení jednotky je nastaveno. Nicméně dokud není aktivováno *uzamykání* jednotky, uživatelé nemusí před přístupem provádět ověření pro jednotku před spuštěním systému Windows.

Ochranu dat jednotky s automatickým šifrováním můžete deaktivovat zde. Když je zakázána, veškeré rozšířené funkce zabezpečení jednotky s automatickým šifrováním jsou vypnuty a jednotka se chová jako standardní disk. Deaktivace ochrany dat také vymaže všechna bezpečnostní nastavení včetně údajů správce jednotky a jejích uživatelů. Tato funkce však nezmění ani neodstraní žádná uživatelská data v jednotce.

Uzamykání
Zobrazuje stav *povoleno* nebo *zakázáno* pro jednotky s automatickým šifrováním. Informace o chování uzamknuté jednotky najdete v tématu Jednotka s automatickým šifrováním.

Může být nutné dočasně zakázat uzamykání jednotky, což můžete provést zde. Zakázání uzamykání jednotky není doporučeno, jelikož v takovém případě není při přístupu k jednotce vyžadováno žádné ověření a k datům může přistupovat jakýkoli uživatel platformy. Při zakázání uzamykání jednotkyjsou zachována veškerá nastavení zabezpečení včetně údajů správce a uživatelů jednotky a veškerých uživatelských dat na jednotce.

POZOR!Pokud chcete odinstalovat aplikaci **Dell Data Protection | Access**, musíte nejprve zakázat ochranu dat jednotky s automatickým šifrováním a odemknout jednotku.

Správce jednotky

Zobrazí aktuálního správce jednotky. Správce jednotky může z tohoto místa určit jiného uživatele jako správce jednotky. Nový správce musí být v systému platný uživatel systému Windows s oprávněními správce. V systému smí existovat pouze jeden správce jednotky.

Uživatelé jednotky

Zobrazí zaregistrované uživatele jednotky a počet aktuálně zaregistrovaných uživatelů. Maximální podporovaný počet uživatelů závisí na jednotce s automatickým šifrováním (aktuálně 4 uživatelé v případě jednotek Seagate a 24 u jednotek Samsung).

Synchronizace s heslem k systému Windows
Funkce synchronizace s heslem k systému Windows (WPS) automaticky nastaví hesla uživatelů jednotky s automatickým šifrováním tak, aby se shodovala s jejich heslem k systému Windows. Tato funkce není vynucována v případě správce jednotky, vztahuje se pouze na uživatele jednotky. Funkci WPS lze použít v podnikových prostředích, kde musí být hesla měněna ve specifických intervalech (např. každých 90 dní). Pokud je tato možnost povolena, hesla k jednotce s automatickým šifrováním všech uživatelů budou při změně hesel k systému Windows automaticky změněna.

POZNÁMKA: Když je synchronizace s heslem k systému Windows povolena (WPS), heslo uživatele jednotky s automatickým šifrováním nelze změnit. Je třeba změnit heslo k systému Windows a heslo k jednotce bude automaticky aktualizováno.

Zapamatovat poslední uživatelské jméno
Když je tato možnost povolena, poslední zadané uživatelské jméno bude v poli **Uživatelské jméno** obrazovky ověření před spuštěním systému Windows zobrazeno jako výchozí.

Výběr uživatelského jména
Když je tato možnost povolena, uživatelé mohou v poli **Uživatelské jméno** obrazovky ověření před spuštěním systému Windows prohlížet jména všech uživatelů jednotky.

Kryptografické vymazání
Tuto možnost lze použít k „vymazání“ veškerých dat na jednotce s automatickým šifrováním. Nedojde ke skutečnému odstranění dat, ale ke smazání klíčů používaných k šifrování dat, což data učiní nepoužitelnými. Po kryptografickém vymazání neexistuje žádný způsob, jak data obnovit. Také bude deaktivována ochrana dat jednotky s automatickým šifrováním a jednotka je připravena k opětovnému použití.

POZNÁMKY:
- Pokud dojde k jakýmkoli problémům týkajícím se funkcí správy jednotky s automatickým šifrováním, zcela vypněte počítač (nerestartujte) a znovu jej spusťte.
- Podrobnější informace o konkrétních chybových zprávách najdete na adrese wave.com/support/Dell.

Informace o ověřovacím zařízení

Okno Informace o ověřovacím zařízení v sekci **Správa zařízení** zobrazuje informace a stav všech ověřovacích zařízení (tj. čtečky otisků prstů, tradiční nebo bezkontaktní čtečky karet Smartcard) připojených k systému.

Technická podpora

Technickou podporu softwaru **Dell Data Protection | Access** najdete na adrese http://www.wave.com/support.dell.com.

CSP na bázi TCG společnosti Wave

Poskytovatel kryptografických služeb (CSP) s technologií Wave Systems Trusted Computing Group (TCG) je součástí aplikace **Dell Data Protection | Access** a je k dispozici pro použití kdykoli je poskytovatel CSP vyžadován – přímo volaný aplikací nebo připravený k výběru ze seznamu nainstalovaných poskytovatelů CSP. Kdykoli je to možné, vybírejte možnost „CSP na bázi TCG společnosti Wave“, aby bylo zajištěno, že budou klíče vytvářeny modulem TPM a že klíče a jejich hesla budou spravovány aplikací **Dell Data Protection | Access**.

Technologie CSP fungující na bázi TCG společnosti Wave Systems umožňuje aplikacím využívat funkce dostupné na platformách v souladu s TCG přímo prostřednictvím MSCAPI. Jedná se o modul MSCAPI CSP podporovaný technologií TCG, který poskytuje asymetrickou funkčnost klíčů na modulu TPM a využívá zvýšenou bezpečnost poskytovanou modulem TPM, bez ohledu na požadavky specifické pro dodavatele týkající se poskytovatele Trusted Software Stuck (TSS).

POZNÁMKA: Pokud klíče TPM vygenerované poskytovatelem CSP na bázi TCG společnosti Wave vyžadují heslo a uživatel vytvořil hlavní heslo TPM, hesla jednotlivých klíčů budou náhodně generována a ukládána ve schránce hesel TPM.