Dell Data Protection | Access — strona główna

Strona główna aplikacji **Dell Data Protection | Access**to miejsce, z którego można uzyskać dostęp do funkcji tej aplikacji. W oknie tym dostępne są następujące funkcje:

System Access Wizard
Opcje dostępu
Self-Encrypting Drive
Opcje zaawansowane

W prawym dolnym rogu okna znajduje się łącze **zaawansowane**, którego kliknięcie powoduje przejście do opcji zaawansowanych.

W oknie opcji zaawansowanych można kliknąć znajdujące się w prawym dolnym rogu łącze **strona główna**, aby powrócić do strony głównej.

System Access Wizard

Kreator System Access Wizard jest otwierany automatycznie przy pierwszym uruchomieniu aplikacji **Dell Data Protection | Access** afişareKreator przeprowadzi użytkownika przez konfigurację wszystkich aspektów zabezpieczeń systemu, w tym metody (npafişaretylko hasło albo linie papilarne i hasło) oraz momentu (w systemie Windows, Pre-Windows lub w obu) logowania użytkownika na komputerzeafişareJeśli komputer jest wyposażony w dysk samoszyfrujący, można go także skonfigurować przy użyciu tego kreatora.

Funkcje administratora

Użytkownicy z uprawnieniami administratora systemu Windows na komputerze mają dostęp do następujących funkcji aplikacji **Dell Data Access | Protection**, które są zablokowane dla zwykłych użytkowników:

- Ustawianie/zmienianie hasła systemowego (Pre-Windows)
- Ustawianie/zmienianie hasła dysku twardego
- Ustawianie/zmienianie hasła administratora
- Ustawianie/zmienianie hasła właściciela układu TPM
- Ustawianie/zmienianie hasła administratora układu ControlVault
- Resetowanie systemu
- Archiwizowanie i przywracanie poświadczeń
- Ustawianie/zmienianie numeru PIN karty smartcard administratora
- Czyszczenie/resetowanie karty smartcard
- Włączanie/wyłączanie bezpiecznego logowania do systemu Windows firmy Dell
- Ustawianie zasad logowania do systemu Windows
- Zarządzanie dyskami samoszyfrującymi, w tym:
    - Włączanie/wyłączanie blokowania dysków samoszyfrujących
    - Włączanie/wyłączanie synchronizacji haseł systemu Windows (Windows Password Synchronization, WPS)
    - Włączanie/wyłączanie rejestracji pojedynczej (Single Sign On, SSO)
    - Przeprowadzanie wymazywania kryptograficznego

Zarządzanie zdalne

W organizacji można skonfigurować środowisko, w którym funkcje zabezpieczeń aplikacji **Dell Data Protection | Access** na wielu platformach są zarządzane centralnie (tznafişarezarządzane zdalnie)afişare W takim przypadku można wykorzystać infrastrukturę zabezpieczeń systemu Windows, taką jak usługi Active Directory, do bezpiecznego zarządzania określonymi funkcjami aplikacji **Dell Data Protection | Access**.

Gdy komputer jest zarządzany zdalnie (npafişare„należy” do administratora zdalnego), funkcje lokalnego administrowania aplikacją **Dell Data Protection | Access** będą wyłączone — okna zarządzania aplikacji nie będą dostępne lokalnieafişareNastępującymi funkcjami można zarządzać zdalnie:

- Trusted Platform Module (TPM)
- ControlVault
- Logowanie Pre-Windows
- Resetowanie systemu
- Hasła systemu BIOS
- Zasady logowania systemu Windows
- Dyski Self-Encrypting Drive
- Rejestrowanie linii papilarnych i kart smartcard

Więcej informacji dotyczących aplikacji Wave Systems EMBASSY® Remote Administration Server (ERAS) do zarządzania zdalnego można uzyskać u przedstawiciela handlowego firmy Dell lub w witrynie internetowej dell.com.

Opcje dostępu

W oknie Opcje dostępu można skonfigurować sposób uzyskiwania dostępu do systemuafişare

Jeśli jakiekolwiek opcje aplikacji **Dell Data Protection | Access** są skonfigurowane, będą one wyświetlane na stronie głównej razem z dostępnymi opcjami (npafişare zmień hasło logowania Pre-Windows)afişareDostępne opcje to skróty, po kliknięciu których otwierane są odpowiednie okna umożliwiające wykonanie konkretnego zadania (npafişarezmiana hasła logowania Pre-Windows lub zarejestrowanie kolejnych linii papilarnych).

Ogólne
Najpierw można określić, kiedy ma następować logowanie (przy uruchomieniu systemu Windows, Pre-Windows lub na obu tych etapach) i w jaki sposób (npafişarelinie papilarne i hasło)afişareMożna wybrać jedną lub dwie opcje sposobu logowaniaafişareDo wyboru są kombinacje wykorzystania linii papilarnych, karty smartcard i hasłaafişareLista opcji zależy od zasad logowania stosowanych w środowisku użytkownika oraz możliwości technicznych danej platformy.

Linie papilarne
Jeśli dany system jest wyposażony w czytnik linii papilarnych, możliwe jest rejestrowanie i aktualizowanie linii papilarnych wykorzystywanych do logowania do systemuafişarePo zarejestrowaniu linii papilarnych palca ich przeskanowanie przez czytnik umożliwia zalogowanie przy lub przed uruchomieniem systemu Windows (zależnie od wybranych ustawień ogólnych opcji dostępu)afişareWięcej informacji można znaleźć w części Rejestrowanie linii papilarnych użytkowników.

Logowanie Pre-Windows
Jeśli wybrano konieczność logowania Pre-Windows, należy skonfigurować hasło systemowe (hasło Pre-Windows)afişarePo jego skonfigurowaniu administrator może w dowolnym momencie zmienić hasłoafişare

Na tym ekranie można również wyłączyć logowanie Pre-Windows (przed uruchomieniem systemu Windows)afişareW tym celu należy podać aktualne hasło systemowe, sprawdzić poprawność hasła, a następnie kliknąć przycisk **Wyłącz**.

Karta smartcard
Jeśli wybrano konieczność logowania się użytkowników przy użyciu kart smartcard, należy zarejestrować co najmniej jedną tradycyjną (wymagającą zetknięcia z czytnikiem) kartę smartcard lub kartę contactless smartcard (bezdotykową)afişareKliknij łącze **Zarejestruj kolejną kartę smartcard**, aby otworzyć kreatora rejestrowania karty smartcardafişareRejestrowanie to konfigurowanie karty smartcard na potrzeby jej wykorzystywania do logowania użytkownika.

Po zarejestrowaniu karty smartcard można zmienić lub skonfigurować jej numer PIN przy użyciu łącza **Zmień lub skonfiguruj numer PIN karty smartcard**.

Logowanie Pre-Windows

Gdy skonfigurowane jest logowanie Pre-Windows, użytkownik musi uwierzytelnić się (przy użyciu hasła, linii papilarnych lub karty smartcard) po uruchomieniu komputera, a przed załadowaniem systemu WindowsafişareLogowanie Pre-Windows zapewnia dodatkowe zabezpieczenie komputera — zapobiega naruszeniu zabezpieczeń systemu Windows i dostępowi do komputera przez nieautoryzowanych użytkowników (npafişarew przypadku kradzieży komputera).

W oknie Logowanie Pre-Windows administratorzy mogą skonfigurować logowanie przed uruchomieniem systemu Windows lub utworzyć albo zmienić hasło Pre-Windows (systemowe)afişareJeśli hasło to zostało już skonfigurowane, w tym oknie można wyłączyć logowanie Pre-WindowsafişareRozpoczęcie konfigurowania logowania Pre-Windows spowoduje otwarcie kreatora umożliwiającego wykonanie następujących czynności:

- Hasło systemowe: skonfigurowanie hasła systemowego (Pre-Windows) dostępu do komputera przed uruchomieniem systemu WindowsafişareTo hasło służy również jako środek awaryjny, gdy użytkownik korzysta z dodatkowych metod uwierzytelniania (npafişareaby umożliwia uzyskanie dostępu do komputera, gdy wystąpi problem z czytnikiem linii papilarnych).
- Linie papilarne lub karta smartcard: skonfigurowanie linii papilarnych lub karty smartcard używanych podczas logowania Pre-Windows oraz określenie, czy ta metoda uwierzytelniania będzie używana zamiast hasła Pre-Windows, czy jako jego uzupełnienie.
- Single Sign On: domyślnie metoda uwierzytelniania Pre-Windows (hasło, linie papilarne lub karta smartcard) będzie też używana do automatycznego logowania do systemu Windows (takie pojedyncze logowanie nosi nazwę „Single Sign On")afişareAby wyłączyć tę funkcję, należy zaznaczyć pole wyboru „Chcę logować się jeszcze raz do systemu Windows".
- Jeśli oprócz hasła Pre-Windows skonfigurowano hasło dysku twardego w systemie BIOS, dostępna będzie również opcja zmiany lub wyłączenia hasła dysku twardego.

UWAGA: Nie wszystkie czytniki linii papilarnych mogą służyć do uwierzytelniania Pre-WindowsafişareJeśli używany czytnik nie jest obsługiwany, możliwe będzie jego wykorzystanie tylko przy logowaniu w systemie WindowsafişareAby uzyskać informacje o zgodności konkretnego czytnika linii papilarnych, należy się skontaktować z administratorem systemu lub przejść do witryny internetowej support.dell.com, gdzie znajduje się lista obsługiwanych czytników linii papilarnych.

Wyłącz logowanie Pre-Windows
W tym oknie można również wyłączyć logowanie Pre-WindowsafişareW tym celu konieczne jest podanie aktualnego hasła Pre-Windows (systemowego)afişareUpewnij się, że hasło jest prawidłowe, a następnie kliknij przycisk **Wyłącz** afişareNależy pamiętać, że po wyłączeniu logowania Pre-Windows wszystkie zarejestrowane linie papilarne i karty smartcard pozostają nadal zarejestrowane.

Rejestrowanie i usuwanie linii papilarnych

Użytkownicy mogą rejestrować i aktualizować linie papilarne, których można używać na komputerze do uwierzytelniania Pre-Windows albo podczas logowania w systemie WindowsafişareNa karcie Linie papilarne wyświetlanie są obrazy dłoni, pokazujące zarejestrowane palceafişareKliknięcie łącza **Zarejestruj kolejny** powoduje otwarcie kreatora rejestrowania linii papilarnych, który przeprowadza użytkownika przez proces rejestracjiafişare„Rejestrowanie" oznacza zapisanie linii papilarnych, które mają być używane do logowaniaafişareAby przeprowadzić rejestrowanie linii papilarnych, należy posiadać prawidłowo zainstalowany i skonfigurowany odpowiedni czytnik linii papilarnych.

UWAGA: Nie wszystkie czytniki linii papilarnych mogą służyć do logowania Pre-WindowsafişareW przypadku próby zarejestrowania linii papilarnych na potrzeby logowania Pre-Windows przy użyciu nieobsługiwanego czytnika wyświetlony zostanie komunikat o błędzieafişareAby uzyskać informacje o zgodności urządzenia, należy się skontaktować z administratorem systemu lub przejść do witryny internetowej support.dell.com, gdzie znajduje się lista obsługiwanych czytników linii papilarnych.

Podczas rejestrowania linii papilarnych wyświetlony zostanie monit o podanie przez użytkownika jego hasła do systemu Windows w celu zweryfikowania tożsamościafişareJeśli wymagają tego stosowane zasady, wyświetlony zostanie również monit o podanie hasła do logowania Pre-Windows (hasła systemowego)afişareHasła tego można użyć w celu uzyskania dostępu do komputera w przypadku problemu z czytnikiem linii papilarnych.

UWAGI:

- Zaleca się zarejestrowanie co najmniej dwóch odcisków linii papilarnych.
- Przed włączeniem uwierzytelniania na podstawie linii papilarnych należy się upewnić, że linie papilarne zostały zarejestrowane prawidłowo.
- W przypadku wymiany czytnika linii papilarnych w komputerze należy ponownie zarejestrować linie papilarne przy użyciu nowego czytnikaafişare Nie zaleca się zamiennego używania dwóch różnych czytników linii papilarnychafişare
- Jeśli podczas rejestrowania linii papilarnych wielokrotnie pojawił się komunikat „czytnik utracił ostrość", możliwe że komputer nie wykrywa czytnika linii papilarnychafişareJeśli czytnik linii papilarnych jest urządzeniem zewnętrznym, jego odłączenie i ponownie podłączenie często rozwiązuje ten problemafişare

Czyszczenie zarejestrowanych linii papilarnych
Zarejestrowane linie papilarne można usunąć, klikając łącze **Usuń linie papilarne** lub klikając (aby usunąć zaznaczenie) zarejestrowany palec w kreatorze rejestrowania linii papilarnych.

Aby usunąć konkretnego użytkownika, który zarejestrował linie papilarne na potrzeby uwierzytelniania Pre-Windows, administrator może usunąć zaznaczenie wszystkich linii papilarnych zarejestrowanych dla tego użytkownika.

UWAGA: Jeśli w trakcie rejestrowania linii papilarnych wystąpią jakiekolwiek błędy, należy zapoznać się z dodatkowymi informacjami w witrynie internetowej wave.com/support/Dell.

Rejestrowanie kart smartcard

Aplikacja **Dell Data Protection | Access** umożliwia używanie tradycyjnych (wymagających zetknięcia z czytnikiem) lub bezdotykowych (contactless) kart smartcard w celu logowania się do konta systemu Windows oraz uwierzytelniania Pre-Windows. Kliknięcie łącza **Zarejestruj kolejną kartę smartcard** na karcie Karta smartcard powoduje otwarcie kreatora rejestrowania karty smartcard, który przeprowadza użytkownika przez proces rejestracjiafişare„Rejestrowanie" oznacza konfigurowanie karty smartcard na potrzeby jej używania w celu logowania użytkownika.

Aby przeprowadzić rejestrowanie, należy posiadać prawidłowo zainstalowane i skonfigurowane odpowiednie urządzenie do uwierzytelniania przy użyciu kart smartcardafişare

UWAGA: Aby uzyskać informacje o zgodności konkretnego urządzenia, należy się skontaktować z administratorem systemu lub przejść do witryny internetowej support.dell.com, gdzie znajduje się lista obsługiwanych kart smartcard.

Rejestracja
Podczas rejestrowania karty smartcard wyświetlony zostanie monit o podanie przez użytkownika jego hasła do systemu Windows w celu zweryfikowania tożsamościafişareJeśli wymagają tego stosowane zasady, wyświetlony zostanie również monit o podanie hasła do logowania Pre-Windows (hasła systemowego)afişareHasła tego można użyć w celu uzyskania dostępu do komputera w przypadku problemu z czytnikiem kart smartcard.

Podczas rejestrowania wyświetlony zostanie monit o podanie numeru PIN karty smartcard (jeśli został on ustawiony)afişareJeśli stosowane zasady wymagają podania numeru PIN, a nie został on ustawiony, wyświetlony zostanie monit o jego utworzenie.

UWAGI:

- Użytkownika nie można usunąć, gdy zostanie zarejestrowany jako używający karty smartcard do logowania Pre-Windows.
- Zwykli użytkownicy mogą zmieniać swój numer PIN na karcie smartcard, a administrator może zmieniać zarówno numer PIN administratora, jak i numery PIN użytkownikówafişare
- Administrator może również zresetować kartę smartcardafişarePo zresetowaniu nie można jej używać do uwierzytelniania podczas logowania do systemu Windows ani logowania Pre-Windows, dopóki nie zostanie zarejestrowana ponownie.

UWAGA: W przypadku uwierzytelniania z użyciem certyfikatu TPM administratorzy mogą rejestrować certyfikaty TPM za pośrednictwem procesu rejestrowania kart smartcard systemu Microsoft WindowsafişareAdministratorzy jako dostawcę usług kryptograficznych muszą wybrać opcję „Wave TCG-Enabled CSP" zamiast dostawcy Smartcard CSP, aby zapewnić zgodność z tą aplikacją. Ponadto musi być włączone bezpieczne logowanie firmy Dell z odpowiednimi zasadami typu uwierzytelniania dla klienta afişare

UWAGA: Jeśli wystąpi błąd z informacją, że usługa Karta inteligentna nie działa, można uruchomić (ponownie) tę usługę w następujący sposób:

- Przejdź z Panelu sterowania do okna Narzędzia administracyjne, wybierz aplet Usługi, a następnie kliknij prawym przyciskiem myszy pozycję Karta inteligentna i wybierz polecenie Uruchom albo Uruchom ponownie.
- Bardziej szczegółowe informacje o konkretnym komunikacie o błędzie są dostępne w witrynie internetowej wave.com/support/Dell.

Dysk Self-Encrypting Drive — przegląd

Aplikacja **Dell Data Protection | Access** służy do zarządzania funkcjami zabezpieczeń sprzętowych dysków samoszyfrujących, w których szyfrowanie danych jest realizowane przez elementy sprzętowe dyskuafişareZadaniem tych funkcji jest zapewnienie, że tylko autoryzowani użytkownicy będą mieć dostęp do zaszyfrowanych danych (po włączeniu blokowania dysku)afişare

Okno Self-Encrypting Drive jest dostępne po kliknięciu dolnej karty **Self-Encrypting Drive** afişareTa karta jest wyświetlana tylko wtedy, gdy w komputerze znajduje się co najmniej jeden dysk samoszyfrujący (SED).

Kliknij łącze **Konfiguracja**, aby otworzyć kreatora konfiguracji dysku Self-Encrypting DriveafişarePrzy użyciu tego kreatora tworzone jest hasło administratora dysku, kopia zapasowa tego hasła oraz ustawienia szyfrowaniaafişareDostęp do kreatora konfiguracji dysku Self-Encrypting Drive mają tylko administratorzy systemuafişare

Ważne! Po skonfigurowaniu dysku ochrona danych oraz blokowanie dysku są „włączone”afişareGdy dysk jest zablokowany:

- Dysk przechodzi w tryb *zablokowany* po każdym wyłączeniu jego zasilania.
- Rozruch z dysku nie nastąpi dopóki użytkownik nie wprowadzi prawidłowej nazwy użytkownika i hasła (lub zeskanuje linii papilarnych) na ekranie logowania Pre-WindowsafişarePrzed włączeniem blokowania dysku znajdujące się na nim dane są dostępne dla wszystkich użytkowników komputera.
- Dysk jest zabezpieczony nawet po podłączeniu do innego komputera jako drugi dysk — aby uzyskać dostęp do danych, konieczne jest uwierzytelnienie.

Po skonfigurowaniu dysku w oknie Self-Encrypting Drive będą wyświetlane dyski oraz łącze umożliwiające użytkownikom zmianę własnego hasła do dyskuafişareAdministrator dysku może również w tym oknie dodawać i usuwać użytkowników dysku. Jeśli dostępny jest skonfigurowany dysk zewnętrzny, będzie on wyświetlany w tym oknie i można będzie go tu odblokowaćafişare

UWAGA: Aby można było zablokować drugi, zewnętrzny dysk, musi on być wyłączany niezależnie od komputera.

Administrator dysku może zarządzać ustawieniami dysku w sekcji **Zaawansowane>Urządzenia** afişareWięcej informacji można znaleźć w temacie Zarządzanie urządzeniami — Self-Encrypting Drives.

Konfiguracja dysku

Kreator konfiguracji dysku Self-Encrypting Drive przeprowadzi użytkownika przez proces konfigurowania dyskówafişareW trakcie tego procesu należy pamiętać znaczenie następujących koncepcji.

Administrator dysku
Pierwszy użytkownik z uprawnieniami administratora systemu, który skonfiguruje dostęp do dysku (i ustawi hasło administratora dysku) staje się administratorem dyskuafişareJest to jedyny użytkownik z prawami do zmieniania ustawień dostępu do dyskuafişareAby zapewnić, że pierwszy użytkownik jest konfigurowany jako administrator dysku w sposób zamierzony, należy zaznaczyć pole wyboru „Rozumiem” przed przejściem dalejafişare

Hasło administratora dysku
W kreatorze zostanie wyświetlony monit o utworzenie hasła administratora dysku i ponowne wprowadzenie tego hasła w celu potwierdzeniaafişareAby móc utworzyć hasło administratora

dysku, użytkownik musi podać swoje hasło do systemu Windows na potrzeby ustalenia jego tożsamościafişareAktualny użytkownik systemu Windows musi mieć prawa administratora, aby utworzyć to hasło.

Utwórz kopię zapasową poświadczeń do dysku
Wpisz lokalizację lub kliknij przycisk **Przeglądaj**, aby wybrać miejsce zapisu kopii zapasowej poświadczeń administratora dyskuafişare

WAŻNE**!**

- Zdecydowanie zaleca się utworzenie kopii zapasowej tych poświadczeń i jej zapisanie na dysku innym niż główny dysk twardy (npafişarena nośniku wymiennym)afişareW przeciwnym razie jeśli dostęp do dysku zostanie utracony, nie będzie możliwy dostęp do kopii zapasowej.
- Po skonfigurowaniu dysku przy następnym uruchomieniu komputera w celu uzyskania dostępu wszyscyużytkownicy będą musieli podać przed załadowaniem systemu Windows prawidłowe nazwy użytkownika i hasła (lub skanować linie papilarne).

Dodaj użytkownika dysku
Administrator dysku może dodawać innych użytkowników dysku, którzy są prawidłowymi użytkownikami systemu WindowsafişarePrzy dodawaniu użytkowników dysku administrator może ustawić wymóg zresetowania przez użytkownika jego hasła podczas pierwszego logowaniaafişareAby odblokować dysk, użytkownik będzie musiał zresetować swoje hasło na ekranie uwierzytelniania Pre-Windows.

Ustawienia zaawansowane

- *Single Sign On* — domyślnie hasło użytkownika do dysku Self-Encrypting Drive, podawane przed uruchomieniem systemu Windows (Pre-Windows), będzie też używane do automatycznego zalogowania użytkownika do systemu Windows (pojedyncze logowanie, tzwafişare„Single Sign On”)afişareAby wyłączyć tę funkcję, zaznacz pole wyboru „Chcę logować się jeszcze raz do systemu Windows” podczas konfigurowania ustawień dysku.
- *Logowanie przy użyciu linii papilarnych* — na platformach obsługujących tę funkcję jako metodę uwierzytelniania do dysku samoszyfrującego zamiast hasła można wybrać skanowanie linii papilarnychafişare
- *Obsługa funkcji Uśpienie/Wstrzymanie (S3)* (jeśli jest obsługiwana na danej platformie) — jeśli ta opcja jest włączona, dysk samoszyfrujący może bezpiecznie przechodzić w tryb uśpienia/wstrzymania (tryb S3), a podczas wznawiania pracy z tego trybu wymagane będzie uwierzytelnienie Pre-Windows.

UWAGI:

- Gdy włączona jest obsługa trybu S3, hasła szyfrowania dysku podlegają wszystkim obowiązującym ograniczeniom haseł systemu BIOSafişareAby uzyskać więcej informacji na temat ograniczeń hasła, które mogą być narzucane przez system BIOS w danym komputerze, należy skontaktować się z producentem komputera.
- Nie wszystkie dyski samoszyfrujące obsługują tryb S3afişarePodczas konfigurowania dysku wyświetlona zostanie informacja, czy dysk obsługuje tryb wstrzymania/uśpieniaafişareW przypadku dysków nieobsługujących tego trybu żądania S3 systemu Windows będą automatycznie przekształcane na żądania hibernacji, jeśli tryb hibernacji jest włączony (zdecydowanie zaleca się włączenie włączenie trybu hibernacji w komputerze).
- Podczas pierwszego logowania po włączeniu opcji Single Sign On (SSO) proces zostanie wstrzymany na ekranie logowania systemu WindowsafişareKonieczne będzie podanie stosowanych poświadczeń uwierzytelniania w systemie Windows, które zostaną bezpiecznie zapisane na potrzeby logowania do systemu Windows w przyszłościafişarePo następnym rozruchu komputera użytkownik zostanie automatycznie zalogowany do

systemu Windows przy użyciu funkcji SSOafişareTaki sam proces jest konieczny także wtedy, gdy metoda uwierzytelniania użytkownika w systemie Windows (hasło, linie papilarne, numer PIN karty smartcard) ulegnie zmianie. Jeśli komputer należy do domeny, a w domenie obowiązują zasady wymagające naciśnięcia klawiszy Ctrl+Alt+Del w celu zalogowania do systemu Windows, zasady te będą przestrzegane.

PRZESTROGA! Jeśli aplikacja **Dell Data Protection | Access** ma zostać odinstalowana, należy najpierw wyłączyć ochronę danych na dysku samoszyfrującym i odblokować dyskafişare

Dyski Self-Encrypting Drive — funkcje użytkownika

Administratorzy dysków samoszyfrujących wykonują wszystkie zadania związane z zarządzaniem zabezpieczeniami i użytkownikami dyskuafişareUżytkownicy dysku, którzy nie są jego administratorami, mogą wykonywać tylko następujące zadania:

- Zmienić swoje własne hasło do dysku.
- Odblokować dysk.

Zadania te są dostępne na karcie **Self-Encrypting Drive** aplikacji **Dell Data Protection | Access**.

Zmień hasło
Funkcja umożliwia zarejestrowanym użytkownikom utworzenie swojego nowego hasła uwierzytelniania dla dyskuafişarePrzed ustawieniem nowego hasła użytkownik musi podać swoje aktualne hasło dysku Self-Encrypting Driveafişare

UWAGI:

- Aplikacja wymusza stosowanie zasad systemu Windows dotyczących długości i złożoności hasła (jeśli są one włączone)afişareJeśli zasady haseł systemu Windows nie są włączone, maksymalna długość hasła dysku Self-Encrypting Drive to 32 znakiafişareNależy pamiętać, że jeśli nie jest włączona funkcjaS3 (Uśpienie/Wstrzymanie), ta maksymalna długość wynosi 127 znaków.
- Hasło użytkownika dysku Self-Encrypting Drive jest inne niż hasło systemu Windows tego użytkownikaafişare Zmiana lub zresetowanie hasła systemu Windows nie ma wpływu na hasło dysku (jeśli nie jest włączona synchronizacja haseł systemu Windows)afişareSzczegółowe informacje można znaleźć w temacie Urządzenia: Self-Encrypting Drive.
- W przypadku niektórych klawiatur z układem innym niż angielski obowiązuje zestaw znaków zastrzeżonych, których nie można używać w haśle dysku samoszyfrującegoafişareJeśli hasło systemu Windows zawiera dowolny ze znaków zastrzeżonych, po włączeniu funkcji synchronizacji haseł systemu Windows synchronizacja nie powiedzie się i zostanie wyświetlony komunikat o błędzie.

Odblokowanie dysku
Funkcja odblokowywania dysku pozwala zarejestrowanemu użytkownikowi odblokować zablokowany dyskafişareJeśli blokowanie dysku jest włączone, dysk przechodzi w stan zablokowany po każdym wyłączeniu zasilania komputeraafişare Po ponownym włączeniu komputera użytkownik musi się uwierzytelnić, podając hasło na ekranie uwierzytelniania Pre-Windows.

UWAGI:

- Przejście w tryb oszczędzania energii (tznafişareUśpienie/Wstrzymanie lub Hibernacja) może być niemożliwe, jeśli równolegle aktywnych na komputerze jest kilka kont użytkowników dysku samoszyfrującego.
- W następujących zlokalizowanych wersjach aplikacji na ekranie uwierzytelniania Pre-Windows nazwy użytkowników dysku są zastąpione nazwami „User 1” (Użytkownik 1), „User 2” (Użytkownik 2) itd.: chińskiej, japońskiej, koreańskiej i rosyjskiej.

Opcje zaawansowane

Opcje zaawansowane aplikacji **Dell Data Protection | Access** pozwalają użytkownikowi z uprawnieniami administratora zarządzać następującymi aspektami aplikacji:

Konserwacja
Hasła
Urządzenia

UWAGA: Tylko użytkownicy z uprawnieniami administratora mogą zmieniać ustawienia opcji zaawansowanychafişareZwykli użytkownicy mogą wyświetlać te ustawienia, ale nie mogą wprowadzać żadnych zmian.

Konserwacja — przegląd

W oknie Konserwacja administratorzy mogą konfigurować preferencje logowania do systemu Windows, resetować system w celu przygotowania go do nowych zadań oraz archiwizować i przywracać poświadczenia użytkowników zapisane w urządzeniach zabezpieczeń sprzętowych komputeraafişareSzczegółowe informacje można znaleźć w następujących tematach:

Preferencje dostępu
Resetowanie systemu
Archiwizowanie i przywracanie poświadczeń

Preferencje dostępu

W oknie Preferencje dostępu administratorzy mogą ustawiać preferencje logowania do systemu Windows dotyczące wszystkich użytkowników systemu.

Włącz bezpieczne logowanie firmy Dell
Ta opcja umożliwia zastąpienie (lub uzupełnienie) standardowego ekranu logowania Ctrl-Alt-Delete systemu Windows inną metodą uwierzytelniania niż hasło dostępu do systemu WindowsafişareJako inną metodę uwierzytelniania można wybrać skanowanie linii papilarnych, co wzmocni zabezpieczenie logowania do systemu WindowsafişareMożna też dodać inne metody, takie jak karty smartcard i certyfikaty TPMafişare

UWAGI:

- Włączenie bezpiecznego logowania firmy Dell dotyczy wszystkich użytkowników systemuafişare
- Zalecane jest włączenie tej opcji PO zarejestrowaniu linii papilarnych lub kart smartcard użytkowników.
- Przy pierwszym logowaniu po włączeniu tej opcji uwierzytelnienie użytkownika w systemie Windows zostanie przeprowadzone przy zastosowaniu standardowych zasad, a po następnym uruchomieniu systemu użyte zostaną nowe metody uwierzytelniania.

Wyłącz bezpieczne logowanie firmy Dell
Ta opcja wyłącza wszystkie funkcje aplikacji **Dell Data Protection | Access** służące do logowania do systemu WindowsafişarePo wybraniu tej opcji zostaną przywrócone standardowe zasady logowania do systemu Windows.

UWAGI:

- Jeśli podczas próby zalogowania wystąpi błąd dotyczący bezpiecznego logowania do systemu Windows, należy wyłączyć i włączyć ponownie opcję bezpiecznego logowania firmy Dell.
- Bardziej szczegółowe informacje o konkretnym komunikacie o błędzie są dostępne w witrynie internetowej wave.com/support/Dell.

Resetowanie systemu

Funkcja resetowania systemu umożliwia wyczyszczenie wszystkich danych użytkowników ze wszystkich urządzeń zabezpieczeń sprzętowych platformyafişareMa ona zastosowanie na przykład podczas przygotowywania komputera do nowych zadańafişareUżycie tej opcji spowoduje wyczyszczenie wszystkich haseł w komputerze z wyjątkiem haseł użytkowników systemu Windows, jak również wszystkich danych w urządzeniach (tznafişareukładach ControlVault i TPM oraz czytnikach linii papilarnych)afişareFunkcja ta wyłącza również ochronę danych na dyskach samoszyfrujących, przez co dane na tych dyskach stają się dostępneafişare.

Należy zatwierdzić zresetowanie komputera, a następnie kliknąć przycisk **Dalej** afişareW celu zresetowania komputera wymagane będzie podanie haseł do wszystkich urządzeń zabezpieczeń sprzętowych (jeśli takie hasła zostały skonfigurowane):

- Właściciela układu TPM
- Administratora układu ControlVault
- Administratora systemu BIOS
- Systemu BIOS (Pre-Windows)
- Dysku twardego (BIOS)
- Administratora dysku Self-Encrypting Drive

UWAGA: Dla dysku samoszyfrującego wymagane jest tylko hasło administratora dysku — nie są wymagane hasła wszystkich użytkowników dysku.

Ważne! Jedyny sposób odzyskania danych wyczyszczonych podczas resetowania komputera to ich przywrócenie z wcześniej zapisanego archiwumafişareJeśli archiwum nie jest dostępne, danych nie można odzyskaćafişareW przypadku dysku samoszyfrującego usuwane są tylko dane konfiguracyjne — nie są usuwane żadne dane osobiste.

Archiwizowanie i przywracanie poświadczeń

Funkcje archiwizowania i przywracanie poświadczeń służą do tworzenia kopii zapasowych oraz przywracania wszystkich poświadczeń użytkowników (danych służących do logowania i szyfrowania) zapisanych w układach ControlVault i Trusted Platform Module (TPM)afişarePosiadanie kopii zapasowej tych danych jest ważne w przypadku ponownego przygotowywania komputera do pracy lub przywracania danych po awarii sprzętuafişareW takiej sytuacji wystarczy przywrócić z zapisanego pliku archiwalnego wszystkie poświadczenia na nowym komputerze.

Można wybrać archiwizację lub przywrócenie poświadczeń jednego użytkownika albo wszystkich użytkowników komputera.

Do poświadczeń użytkownika należą dane używane do logowania Pre-Windows, takie jak zarejestrowane linie papilarne i dane kart smartcard oraz klucze zapisane w układzie TPMafişareUkład TPM tworzy klucze na żądanie bezpiecznych aplikacji, na przykład podczas generowania certyfikatu cyfrowego.

UWAGA: Aby ustalić, czy klucze z układu TPM można archiwizować przy użyciu aplikacji **Dell Data Protection | Access**, zapoznaj się z dokumentacją danej bezpiecznej aplikacjiafişare Ogólnie w przypadku aplikacji generujących klucze przy użyciu dostawcy „Wave TCG-Enabled CSP” jest to możliwe.

Archiwizowanie poświadczeń
Aby zarchiwizować poświadczenia:

- Określ, czy chcesz zarchiwizować własne poświadczenia, czy poświadczenia wszystkich użytkowników komputera.
- Podaj dane uwierzytelniania dla zabezpieczeń sprzętowych, wprowadzając hasło systemowe (Pre-Windows), hasło administratora układu ControlVault i hasło właściciela układu TPM.
- Utwórz hasło kopii zapasowej poświadczeńafişare
- Wybierz lokalizację archiwum, korzystając z przycisku **Przeglądaj** afişare W celu zabezpieczenia przed skutkami awarii dysku twardego jako lokalizację archiwum należy wybrać nośnik wymienny, taki jak dysk flash USB lub dysk sieciowyafişare

Ważne uwagi:

- Należy zanotować informację o lokalizacji archiwum, ponieważ użytkownik będzie jej potrzebować, aby przywrócić dane poświadczeńafişare
- Należy zanotować hasło kopii zapasowej poświadczeń, aby zagwarantować możliwość przywrócenia danychafişareJest to ważne, ponieważ tego hasła nie można odzyskaćafişare
- Jeśli hasło właściciela układu TPM nie jest znane, należy się skontaktować z administratorem systemu albo zapoznać z instrukcją konfigurowania układu TPM komputera.

Przywracanie poświadczeń
Aby przywrócić poświadczenia:

- Określ, czy chcesz przywrócić własne poświadczenia, czy poświadczenia wszystkich użytkowników komputera.
- Przejdź do lokalizacji archiwum i wybierz plik archiwumafişare
- Podaj hasło kopii zapasowej poświadczeń, które utworzono podczas tworzenia archiwum.

- Podaj dane uwierzytelniania dla zabezpieczeń sprzętowych, wprowadzając hasło systemowe (Pre-Windows), hasło administratora układu ControlVault i hasło właściciela układu TPM.

UWAGI:

- Jeśli wystąpi błąd z informacją, że przywracanie poświadczeń nie powiodło się, a podjęto wiele prób przywracania, należy spróbować przywrócić dane z innego pliku archiwumafişareJeśli to się nie uda, należy utworzyć nowe archiwum poświadczeń i spróbować przywrócić dane z tego nowego archiwum.
- Jeśli wystąpi błąd z informacją, że nie udało się przywrócić kluczy układu TPM, należy utworzyć archiwum poświadczeń, a następnie wyczyścić układ TPM w systemie BIOSafişareAby wyczyścić układ TPM, uruchom ponownie komputer, podczas rozpoczynania tworzenia kopii zapasowej naciśnij klawisz **F2**, aby przejść do ustawień systemu BIOS, a następnie przejdź do opcji Security (Zabezpieczenia) > TPM Security (Zabezpieczenia układu TPM)afişareNastępnie ponownie ustanów prawo własności układu TPM i spróbuj ponownie przywrócić poświadczenia.
- Bardziej szczegółowe informacje o konkretnym komunikacie o błędzie są dostępne w witrynie internetowej wave.com/support/Dell.

Zarządzanie hasłami

W oknie Zarządzanie hasłami administrator może tworzyć i zmieniać wszystkie hasła zabezpieczeń w komputerze:

- Systemowe (Pre-Windows)*
- Administratora*
- Dysku twardego*
- ControlVault
- Właściciela układu TPM
- Główne układu TPM
- Magazynu haseł TPM
- Dysku Self-Encrypting Drive

UWAGI:

- Wyświetlane będą tylko hasła mające zastosowanie w aktualnej konfiguracji platformyafişareDlatego zawartość tego okna będzie się zmieniać w zależności od konfiguracji i stanu komputera.
- Hasła oznaczone gwiazdką (*) to hasła systemu BIOS, które można zmienić również w systemie BIOS komputera.
- Haseł z poziomu systemu BIOS nie można tworzyć ani zmieniać, jeśli administrator systemu BIOS uniemożliwił zmienianie hasełafişare
- Kliknięcie łącza **konfiguracja** dla dysku samoszyfrującego powoduje otwarcie kreatora Self-Encrypting Drive WizardafişareKliknięcie łącza **zarządzaj** umożliwia użytkownikowi zmienienie jednego lub więcej haseł dysków samoszyfrujących.
- Kliknięcie łącza **zarządzaj** dla magazynu haseł TPM powoduje wyświetlenie okna, w którym można wyświetlić lub zmienić hasła chroniące klucze TPMafişarePodczas tworzenia klucza TPM wymagającego hasła hasło jest generowane losowo i umieszczane w magazynieafişareMagazynem haseł TPM nie można zarządzać, jeśli nie utworzono hasła głównego układu TPMafişare

Reguły złożoności hasła systemu Windows

Aplikacja **Dell Data Protection | Access** zapewnia, że następujące hasło jest zgodne z regułami złożoności hasła w systemie Windows na danym komputerze:

- Hasło właściciela układu TPM

W celu określenia zasad złożoności hasła dla danego komputera:

1. Otwórz Panel sterowania.
2. Kliknij dwukrotnie ikonę Narzędzia administracyjne.
3. Kliknij dwukrotnie opcję Lokalna zasada zabezpieczeń.
4. Rozwiń opcję Zasady kont i wybierz opcję Zasady haseł.

Urządzenia — przegląd

W oknie Urządzenia administratorzy mogą zarządzać wszystkimi zabezpieczeniami sprzętowymi zainstalowanymi w systemieafişareDla każdego urządzenia można wyświetlić informacje o stanie oraz inne informacje szczegółowe, takie jak wersja oprogramowania układowegoafişareKliknięcie opcji **pokaż** powoduje wyświetlenie informacji o każdym z urządzeń, a kliknięcie opcji **ukryj** — zwinięcie tej sekcjiafişareZarządzać można następującymi urządzeniami (w zależności od tego, jakie urządzenia są zainstalowane):

Układ Trusted Platform Module (TPM)
Układ ControlVault®
Dyski Self-Encrypting Drive
Informacje o urządzeniach do uwierzytelniania

Trusted Platform Module (TPM)

Aby korzystać z zaawansowanych funkcji zabezpieczeń dostępnych w aplikacji **Dell Data Protection | Access** i układzie TPM, elektroniczny układ zabezpieczeń sprzętowych TPM musi być włączony oraz musi być skonfigurowany właściciel układu TPM.

Okno Trusted Platform Module w sekcji **Zarządzanie urządzeniami** jest wyświetlane tylko wtedy, gdy w komputerze wykryty zostanie układ TPM.

Zarządzanie układem TPM

Te funkcje umożliwiają administratorom systemu zarządzanie układem TPMafişare

Stan

Wyświetla informacje o stanie (*aktywny* lub *nieaktywny*) układu TPMafişareStan „aktywny" oznacza, że układ TPM jest włączony w systemie BIOS i jest gotowy do skonfigurowania (tznafişaremożna nadać mu właściciela)afişareUkładem TPM nie można zarządzać, a jego funkcje zabezpieczeń nie są dostępne, jeśli układ TPM nie jest aktywny (włączony).

Jeśli w komputerze wykryto układ TPM, ale nie jest on aktywny (włączony), można go włączyć, klikając łącze **aktywuj** w tym oknie (nie ma konieczności przechodzenia do systemu BIOS)afişarePo włączeniu układu TPM przy użyciu tej funkcji należy ponownie uruchomić komputerafişarePodczas ponownego uruchamiania w niektórych przypadkach zostanie wyświetlony monit o zaakceptowanie zmianafişare

UWAGA: Włączenie (aktywowanie) układu TPM przy użyciu tej aplikacji może nie być obsługiwane na wszystkich platformachafişareW takim przypadku konieczne jest jej włączenie w systemie BIOS komputeraafişareW tym celu uruchom ponownie komputer, przed rozpoczęciem ładowania systemu Windows naciśnij klawisz **F2**, aby przejść do konfiguracji systemu BIOS, a następnie przejdź do obszaru Security (Zabezpieczenia) > TPM Security (Zabezpieczenia układu TPM) i aktywuj układ TPM.

W tym miejscu można również *dezaktywować* układ TPM, klikając łącze **dezaktywuj**afişareDezaktywowanie układu TPM spowoduje, że będzie on niedostępny do wykorzystania przez zaawansowane funkcje zabezpieczeńafişareDezaktywacja nie powoduje jednak zmiany żadnych ustawień układu TPM ani usunięcia czy zmodyfikowania żadnych informacji i kluczy zapisanych w układzie TPM.

Ustanowione prawo własności

Wyświetla stan prawa własności (tznafişare„ma właściciela") i umożliwia ustanowienie lub zmianę właściciela układu TPMafişarePrawo własności układu TPM musi być ustanowione, aby dostępne były funkcje zabezpieczeń tego układuafişareAby można było ustanowić prawo własności układu TPM, układ musi być włączony (aktywowany)afişare

Na proces ustanawiania prawa własności składa się utworzenie przez użytkownika (z uprawnieniami administratora) hasła właściciela układu TPMafişare Po określeniu hasła prawo własności zostaje ustanowione i układ TPM jest gotowy do użytkuafişare

UWAGA: Hasło właściciela układu TPM musi być zgodne z regułami złożoności haseł systemu Windows obowiązującymi na komputerzeafişare

Ważne! Ważne jest, aby nie stracić ani nie zapomnieć hasła właściciela układu TPM, ponieważ jest ono konieczne, aby mieć dostęp do zaawansowanych funkcji zabezpieczeń układu TPM w aplikacji **Dell Data Protection | Access**.

Zablokowany
Wyświetla informacje o stanie (*zablokowany* lub *odblokowany*) układu TPMafişare„Blokowanie” to funkcja zabezpieczeń układu TPMafişareUkład TPM przejdzie w stan zablokowany po określonej liczbie prób wprowadzenia nieprawidłowego hasła właściciela układu TPMafişareWłaściciel układu TPM może odblokować ten układ w tym miejscuafişareKonieczne jest podanie hasła właściciela układu TPM.

UWAGI:

- Jeśli wystąpi błąd z informacją, że nie udało się ustanowić prawa własności do układu TPM, należy wyczyścić układ TPM w systemie BIOS komputera i spróbować ponownie ustanowić prawo własnościafişareAby wyczyścić układ TPM, uruchom ponownie komputer, podczas rozpoczynania tworzenia kopii zapasowej naciśnij klawisz **F2**, aby przejść do ustawień systemu BIOS, a następnie przejdź do opcji Security (Zabezpieczenia) > TPM Security (Zabezpieczenia układu TPM).
- Jeśli wystąpi błąd z informacją, że nie można zmienić hasła właściciela układu TPM, zarchiwizuj dane z układu TPM (archiwizowanie poświadczeń), wyczyść układ TPM w systemie BIOS, ponownie ustanów prawo własności układu TPM i przywróć dane z układu TPM (przywróć poświadczenia)afişare
- Bardziej szczegółowe informacje o konkretnym komunikacie o błędzie są dostępne w witrynie internetowej wave.com/support/Dell.

Dell ControlVault®

Dell ControlVault® (CV) to bezpieczny sprzętowy magazyn poświadczeń użytkowników używanych podczas logowania Pre-Windows (npafişarehaseł użytkowników i zarejestrowanych danych o liniach papilarnych)afişareOkno ControlVault w narzędziu **Zarządzanie urządzeniami** jest wyświetlane, tylko gdy w komputerze zostanie wykryty układ ControlVault.

Zarządzanie układem ControlVault

Opisane funkcje umożliwiają administratorowi systemu zarządzanie układem ControlVault komputera.

Stan
Wyświetla informacje o stanie (*aktywny* lub *nieaktywny*) układu ControlVaultafişareStan „nieaktywny" oznacza, że układ ControlVault jest w komputerze niedostępny jako magazynafişareZapoznaj się z dokumentacją komputera firmy Dell, aby ustalić, czy jest on wyposażony w układ ControlVault.

Hasło
Wskazuje, czy utworzono Hasło administratora układu ControlVault, oraz umożliwia utworzenie lub zmienienie hasła (jeśli zostało ono utworzone wcześniej)afişareTylko administratorzy systemu mogą utworzyć i zmieniać to hasłoafişareUtworzenie hasła administratora układu ControlVault jest konieczne, aby:

- Przeprowadzić archiwizowanie lub przywracanie poświadczeń.
- Wyczyścić dane użytkowników (wszystkich)afişare

UWAGA: Jeśli próba archiwizowania lub przywracania zostanie podjęta, gdy nie utworzono hasła administratora układu ControlVault, zostanie wyświetlony monit o utworzenie tego hasła (jeśli użytkownik jest administratorem).

Zarejestrowani użytkownicy
Wskazuje, czy jacyś użytkownicy zarejestrowali poświadczenia logowania (npafişarehasła, linie papilarne lub dane kart smartcard) obecnie zapisane w układzie ControlVaultafişare

Wyczyść dane użytkowników
Czasem może zaistnieć potrzeba wyczyszczenia danych w układzie ControlVault, na przykład jeśli użytkownicy mają problemy z używaniem lub rejestrowaniem poświadczeń służących do uwierzytelniania Pre-WindowsafişareW tym oknie można wyczyścić wszystkie dane zapisane w układzie ControlVault (dane jednego użytkownika lub wszystkich użytkowników).

Aby wyczyścić dane wszystkich użytkowników platformy, należy wprowadzić hasło administratora układu ControlVaultafişareWyświetlony zostanie również monit o podanie hasła systemowego (Pre-Windows), jeśli zarejestrowane są poświadczenia uwierzytelniania przed uruchomieniem systemu WindowsafişarePodczas czyszczenia danych wszystkich użytkowników resetowane jest hasło administratora układu ControlVault oraz hasło systemoweafişareNależy pamiętać, że jest to jedyny sposób wyczyszczenia hasła administratora układu ControlVault.

UWAGA: Po wyczyszczeniu danych wszystkich użytkowników wyświetlony zostanie monit o ponowne uruchomienie komputeraafişarePonowne uruchomienie jest ważne dla prawidłowego działania komputera.

Aby wyczyścić poświadczenia jednego użytkownika, nie jest konieczne utworzenie hasła administratora układu ControlVaultafişarePo kliknięciu opcji **wyczyść dane użytkownika** wyświetlony zostanie monit o wybranie użytkownika, którego poświadczenia w układzie ControlVault mają zostać wyczyszczoneafişarePo wybraniu użytkownika wyświetlony zostanie

monit o podanie hasła systemowego (tylko jeśli zarejestrowane są poświadczenia logowania Pre-Windows).

UWAGI:

- Jeśli wystąpi błąd z informacją, że nie można utworzyć hasła administratora układu ControlVault, należy zarchiwizować poświadczenia, wyczyścić dane wszystkich użytkowników w układzie ControlVault, ponownie uruchomić komputer i ponownie spróbować utworzyć hasło.
- Jeśli wystąpi błąd z informacją, że nie można wyczyścić poświadczeń jednego użytkownika w układzie ControlVault, należy zarchiwizować poświadczenia, spróbować wyczyścić dane wszystkich użytkowników, a następnie ponownie spróbować wyczyścić dane tego jednego użytkownika.
- Jeśli wystąpi błąd z informacją, że nie można wyczyścić poświadczeń wszystkich użytkowników w układzie ControlVault, należy rozważyć zresetowanie systemuafişare**Ważne!** Przed przeprowadzeniem resetowania należy uważnie zapoznać się z tematem pomocy Resetowanie systemu, ponieważ spowoduje ono wyczyszczenie WSZYSTKICH danych użytkowników związanych z zabezpieczeniami.
- Jeśli wystąpi błąd z informacją, że nie można utworzyć kopii zapasowej danych układów ControlVault i TPM, należy wyłączyć układ TPM w systemie BIOS komputeraafişareW tym celu uruchom ponownie komputer, podczas rozpoczynania tworzenia kopii zapasowej naciśnij klawisz **F2**, aby przejść do ustawień systemu BIOS, a następnie przejdź do opcji Security (Zabezpieczenia) > TPM Security (Zabezpieczenia układu TPM)afişareNastępnie ponownie włącz układ TPM i ponownie spróbuj zarchiwizować dane z układu ControlVault.
- Bardziej szczegółowe informacje o konkretnym komunikacie o błędzie są dostępne w witrynie internetowej wave.com/support/Dell.

Dysk Self-Encrypting Drive: zaawansowane

Aplikacja **Dell Data Protection | Access** służy do zarządzania funkcjami zabezpieczeń sprzętowych dysków samoszyfrujących, w których szyfrowanie danych jest realizowane przez elementy sprzętowe dyskuafişareZadaniem tych funkcji zarządzania jest zapewnienie, że tylko autoryzowani użytkownicy będą mieć dostęp do zaszyfrowanych danych po włączeniu blokowania dysku.

Okno Self-Encrypting Drive w sekcji **Zarządzanie urządzeniami** jest wyświetlane tylko wtedy, gdy w komputerze znajduje się co najmniej jeden dysk samoszyfrujący (SED).

Ważne! Po skonfigurowaniu dysku ochrona danych na dysku samoszyfrującym oraz blokowanie dysku są „włączone”afişare

Zarządzanie dyskiem

Te funkcje umożliwiają administratorowi dysku zarządzanie ustawieniami zabezpieczeń dysku. Zmiany w ustawieniach zabezpieczeń dysku zaczynają obowiązywać po jego wyłączeniu.

Ochrona danych

Wyświetla stan (*włączona* lub *wyłączona*) ochrony danych na dysku samoszyfrującymafişareStan „włączona” oznacza, że zabezpieczenia dysku zostały skonfigurowaneafişareJednak do momentu włączenia *blokowania* dysku użytkownicy nie będą musieć uwierzytelniać się przed uruchomieniem systemu Windows (Pre-Windows), aby uzyskać do niego dostęp.

Tutaj można wyłączyć ochronę danych na dysku samoszyfrującymafişareGdy ochrona jest wyłączona, wszystkie zaawansowane funkcje zabezpieczeń dysku samoszyfrującego są wyłączone, a dysk działa jak zwykły dyskafişareWyłączenie ochrony danych powoduje również usunięcie wszystkich ustawień zabezpieczeń, w tym poświadczeń administratora i użytkowników dyskuafişareFunkcja jednak nie zmienia ani nie usuwa znajdujących się na dysku danych użytkownikówafişare

Blokowanie

Wyświetla stan (*włączone* lub *wyłączone*) blokady dysków samoszyfrującychafişareInformacje o sposobie działania zablokowanego dysku można znaleźć w temacie Self-Encrypting Drive.

Konieczne może być tymczasowe wyłączenie blokowania dysku, co można zrobić tutajafişareNie jest to zalecane, ponieważ przy wyłączonym blokowaniu w celu uzyskania dostępu do dysku nie będzie wymagane podanie żadnych poświadczeń, więc każdy użytkownik będzie mieć dostęp do zawartych na nim danychafişareWyłączenie blokowania dysku nie powodujeusunięcia żadnych ustawień zabezpieczeń, w tym poświadczeń administratora i użytkowników dysku ani danych użytkowników zapisanych na dyskuafişare

PRZESTROGA! Jeśli aplikacja **Dell Data Protection | Access** ma zostać odinstalowana, należy najpierw wyłączyć ochronę danych na dysku samoszyfrującym i odblokować dyskafişare

Administrator dysku

Wyświetla informację o aktualnym administratorze dyskuafişareTutaj administrator dysku może zmienić użytkownika wybranego jako administratorafişareNowy administrator musi być prawidłowym użytkownikiem systemu Windows na komputerze i mieć uprawnienia administracyjneafişareNa komputerze może być tylko jeden administrator dysku.

Użytkownicy dysku

Wyświetla informacje o zarejestrowanych użytkownikach dysku oraz liczbie aktualnie zarejestrowanych użytkownikówafişareMaksymalna liczba użytkowników zależy od rodzaju dysku samoszyfrującego (obecnie 4 użytkowników w przypadku dysków Seagate i 24 użytkowników w przypadku dysków Samsung).

Synchronizacja haseł systemu Windows

Funkcja Synchronizacja haseł systemu Windows (Windows Password Sync, WPS) służy do automatycznego ustawiania haseł użytkowników dysku Self-Encrypting Drive identycznych jak ich hasła w systemie WindowsafişareSynchronizacja ta nie jest wymuszana w przypadku administratora, jest stosowana tylko względem użytkowników dyskuafişareFunkcji WPS można używać w środowiskach korporacyjnych, w których hasła muszą być zmieniane co określony czas (npafişareco 90 dni)afişareGdy ta opcja jest włączona, hasła wszystkich użytkowników dysku samoszyfrującego będą aktualizowane automatycznie, gdy zmienione zostaną ich hasła w systemie Windows.

UWAGA: Gdy synchronizacja haseł systemu Windows (WPS) jest włączona, hasła użytkownika dysku Self-Encrypting Drive nie można zmienićafişareAby automatycznie zaktualizować hasło do dysku, należy zmienić hasło użytkownika w systemie Windows.

Zapamiętuj ostatnią nazwę użytkownika

Gdy ta opcja jest włączona, ostatnia wprowadzona nazwa użytkownika będzie wyświetlana jako domyślna w polu **Nazwa użytkownika** na ekranie uwierzytelniania Pre-Windows.

Wybieranie nazwy użytkownika

Gdy ta opcja jest włączona, użytkownicy mogą wyświetlać nazwy wszystkich użytkowników dysku w polu **Nazwa użytkownika** na ekranie uwierzytelniania Pre-Windowsafişare

Wymazywanie kryptograficzne

Ta opcja służy do „wymazywania” wszystkich danych z dysku samoszyfrującego. Nie powoduje to faktycznego wymazania danych, ale usuwa klucze używane do szyfrowania danych, przez co dane stają się bezużyteczneafişareNie istnieje sposób odzyskania danych z dysku po wymazaniu kryptograficznymafişarePonadto ochrona danych na dysku samoszyfrującym zostaje wyłączona i dysk jest gotowy do przygotowania do nowych zadańafişare

UWAGI:

- Jeśli wystąpią jakiekolwiek błędy związane z funkcjami zarządzania dyskiem samoszyfrującym, całkowicie wyłącz komputer (nie restartuj), a następnie uruchom go ponownie.
- Bardziej szczegółowe informacje o konkretnym komunikacie o błędzie są dostępne w witrynie internetowej wave.com/support/Dell.

Informacje o urządzeniach do uwierzytelniania

W oknie Informacje o urządzeniach do uwierzytelniania narzędzia **Zarządzanie urządzeniami** wyświetlane są informacje o wszystkich podłączonych urządzeniach do uwierzytelniania (tjafişareczytnikach linii papilarnych oraz czytnikach tradycyjnych kart smartcard i kart contactless smartcard (bezdotykowych)) oraz informacje o ich stanie.

Pomoc techniczna

Pomoc techniczna dla oprogramowania **Dell Data Protection | Access** jest dostępna w witrynie internetowej http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP

Dostawca usług kryptograficznych Wave Systems Trusted Computing Group (TCG)-enabled Cryptographic Service Provider (CSP) jest dołączony do aplikacji **Dell Data Protection | Access** i jest zawsze dostępny do użycia, gdy wymagany jest dostawca usług kryptograficznych: wywoływany bezpośrednio z aplikacji lub wybierany z listy zainstalowanych dostawcówafişare Gdy jest to możliwe, należy wybierać opcję „Wave TCG-Enabled CSP”, aby zapewnić, że klucze generuje układ TPM, oraz że do zarządzania kluczami i ich hasłami używana jest aplikacja **Dell Data Protection | Access**.

Dostawca usług kryptograficznych Wave Systems TCG-enabled CSP pozwala aplikacjom wykorzystywać funkcje dostępne na platformach zgodnych ze standardem TCG bezpośrednio przy użyciu interfejsu MSCAPIafişare Jest to moduł dostawcy CSP interfejsu MSCAPI rozbudowany o funkcje TCG, który zapewnia obsługę kluczy asymetrycznych w układzie TPM i umożliwia wykorzystanie rozszerzonych funkcji zabezpieczeń oferowanych przez układ TPM, niezależnie od wymagań dotyczących dostawcy oprogramowania Trusted Software Stack (TSS) specyficznych dla producenta sprzętu.

UWAGA: Jeśli klucze TPM wygenerowane przez dostawcę Wave TCG-enabled CSP wymagają hasła, a użytkownik utworzył hasło główne układu TPM, hasła poszczególnych kluczy będą generowane losowo i zapisywane w magazynie haseł układu TPM.