HP Client Security

Rozpoczęcie pracy

© Copyright 2013 Hewlett-Packard Development Company, L.P.

Bluetooth jest znakiem towarowym należącym do swojego właściciela, używanym przez firmę Hewlett-Packard Company w ramach licencji. Intel jest znakiem towarowym firmy Intel Corporation w USA i innych krajach i jest wykorzystywany na podstawie licencji. Microsoft i Windows są zastrzeżonymi w Stanach Zjednoczonych znakami towarowymi firmy Microsoft Corporation.

Informacje zawarte w niniejszym dokumencie mogą zostać zmienione bez powiadomienia. Jedyne warunki gwarancji na produkty i usługi firmy HP są ujęte w odpowiednich informacjach o gwarancji towarzyszących tym produktom i usługom. Żadne z podanych tu informacji nie powinny być uznawane za jakiekolwiek gwarancje dodatkowe. Firma HP nie ponosi odpowiedzialności za błędy techniczne lub wydawnicze ani pominięcia, jakie mogą wystąpić w tekście.

Wydanie pierwsze: sierpień 2013

Numer katalogowy dokumentu: 735339-241

Spis treści

1 Wprowadzenie do programu HP Client Security Manager 1

Funkcje oprogramowania HP Client Security 1

HP Client Security – opis produktu i przykłady wykorzystania 3

Dostęp do programu Password Manager 4

HP Drive Encryption (tylko wybrane modele) 4

HP Device Access Manager (tylko wybrane modele) 5

Usługa Computrace (do oddzielnego zakupu) 5

Osiągnięcie kluczowych celów bezpieczeństwa 6

Ochrona przed zaplanowaną kradzieżą 6

Ograniczenie dostępu do danych poufnych 6

Uniemożliwienie nieuprawnionego dostępu z lokalizacji wewnętrznych i zewnętrznych 6

Tworzenie mocnych haseł 7

Dodatkowe elementy bezpieczeństwa 7

Przypisywanie ról bezpieczeństwa 7

Zarządzanie hasłami w pakiecie HP Client Security 8

Tworzenie bezpiecznego hasła 8

Tworzenie kopii zapasowej danych uwierzytelniających i ustawień 9

2 Rozpoczęcie pracy 10

Uruchamianie programu HP Client Security 11

3 Instrukcja prostej instalacji dla małych firm 12

Rozpoczęcie pracy 12

Dostęp do programu Password Manager 12

Wyświetlanie i zarządzanie zapisanymi w programie Password Manager danymi uwierzytelniającymi. 13

HP Device Access Manager 13

HP Drive Encryption 13

4 HP Client Security 14

Aplikacje, funkcje i ustawienia tożsamości 14

Linie papilarne 15

Ustawienia administracyjne linii papilarnych 15

Ustawienia użytkownika linii papilarnych 16

HP SpareKey — Odzyskiwanie hasła 16

HP SpareKey Settings 16

hasło systemu Windows 17
Urządzenia Bluetooth 17
Ustawienia urządzeń Bluetooth 17
Karty 18
Ustawienia kart zbliżeniowych, bezstykowych i inteligentnych 19
PIN 19
PIN Settings (Ustawienia systemu BIOS) 20
RSA SecurID 20
Dostęp do programu Password Manager 20
Dla stron internetowych i programów, dla których nie zdefiniowano jeszcze danych logowania. 21
Dla stron internetowych i programów, dla których już zdefiniowano dane logowania. 21
Dodawanie danych logowania 22
Edytowanie danych logowania 23
Korzystanie z menu Quick Links programu Password Manager 23
Tworzenie kategorii danych logowania 24
Zarządzanie danymi logowania 24
Ocena siły hasła 25
Ustawienia ikony programu Password Manager 25
Importowanie i eksportowanie danych logowania 26
Ustawienia 27
Ustawienia zaawansowane 28
Zasady administratora 28
Zasady zwykłego użytkownika 29
Opcje zabezpieczeń 29
Użytkownicy 30
Moje zasady 30
Tworzenie kopii zapasowych i odzyskiwanie danych 31

5 HP Drive Encryption (tylko wybrane modele) 33
Otwieranie narzędzia Drive Encryption 33
Zadania ogólne 34
Aktywacja narzędzia Drive Encryption dla standardowych dysków twardych 34
Aktywacja narzędzia Drive Encryption dla dysków samoszyfrujących 34
Dezaktywacja narzędzia Drive Encryption 35
Logowanie po aktywacji narzędzia Drive Encryption 35
Szyfrowanie dodatkowych dysków twardych 36
Zadania zaawansowane 37
Zarządzanie narzędziem Drive Encryption (zadanie administratora) 37

Szyfrowanie lub deszyfrowanie pojedynczych partycji dyskowych (tylko szyfrowanie programowe) ... 37
Zarządzanie dyskiem ... 37
Kopia zapasowa i odzyskiwanie (zadanie administratora) ... 38
Tworzenie kopii zapasowej kluczy szyfrowania ... 38
Odzyskiwanie dostępu do komputera za pomocą kluczy zapasowych ... 38
Przeprowadzanie odzyskiwania HP SpareKey Recovery ... 39

6 HP File Sanitizer (tylko wybrane modele) ... 40
Niszczenie ... 40
Czyszczenie przestrzeni dyskowej ... 40
Otwieranie narzędzia File Sanitizer ... 41
Procedury konfiguracji ... 41
Ustawienie harmonogramu niszczenia ... 42
Ustawienie harmonogramu czyszczenia przestrzeni dyskowej ... 43
Ochrona plików przed zniszczeniem ... 43
Zadania ogólne ... 44
Użycie ikony programu File Sanitizer ... 44
Niszczenie za pomocą prawego przycisku ... 44
Ręczne uruchamianie operacji niszczenia ... 45
Ręczne uruchamianie czyszczenia przestrzeni dyskowej ... 45
Przeglądanie plików dziennika ... 45

7 HP Device Access Manager (tylko wybrane modele) ... 47
Uruchamianie programu Device Access Manager ... 47
Widok użytkownika ... 48
Widok systemu ... 48
Konfiguracja JITA ... 49
Tworzenie zasad dostępu JITA dla użytkownika lub grupy użytkowników ... 50
Dezaktywacja dostępu JITA dla użytkownika lub grupy użytkowników ... 50
Ustawienia ... 50
Nieobsługiwane klasy urządzeń ... 50

8 HP Trust Circle ... 52
Uruchamianie narzędzia Trust Circles ... 52
Rozpoczęcie pracy ... 52
Trust Circles ... 53
Dodawanie folderów do kręgu zaufania ... 53
Dodawanie członków do kręgu zaufania ... 54

Dodawanie plików do kręgu zaufania 54
Foldery zaszyfrowane 55
Usuwanie folderów z kręgu zaufania 55
Usuwanie pliku z kręgu zaufania 55
Usuwanie członków z kręgu zaufania 55
Usuwanie kręgu zaufania 56
Ustawienia preferencji 56

9 Odzyskiwanie sprzętu po kradzieży (tylko wybrane modele) 58

10 Wyjątki dla lokalizowania haseł 59
Co robić, gdy hasło zostanie odrzucone 59
Edytory IME systemu Windows nie są obsługiwane podczas uwierzytelniania przedrozruchowego i z poziomu programu Drive Encryption. 59
Zmiana hasła za pomocą klawiatury o innym, lecz obsługiwanym układzie 60
Obsługa klawiszy specjalnych 60

Glosariusz 63

Indeks 67

1 Wprowadzenie do programu HP Client Security Manager

Oprogramowanie HP Client Security pozwala na ochronę danych, urządzeń i tożsamości, zwiększając przez to bezpieczeństwo twojego komputera.

Moduły oprogramowania HP Client Security zainstalowana na danym komputerze mogą się różnić w zależności od modelu.

Moduły oprogramowania HP Client Security mogą być zainstalowane fabrycznie, umieszczone i gotowe do zainstalowania na komputerze, lub dostępne do pobrania z witryny HP. Więcej informacji można znaleźć w rozdziale http://www.hp.com.

UWAGA: Wszelkie instrukcje zamieszczone w niniejszym Przewodniku zostały utworzone przy założeniu, że stosowne moduły oprogramowania HP Client Security zostały wcześniej zainstalowane na komputerze.

Funkcje oprogramowania HP Client Security

Poniższa tabela zawiera szczegółowe informacje dotyczących kluczowych funkcji poszczególnych modułów oprogramowania HP Client Security.

Moduł	Funkcje kluczowe
HP Client Security Manager	Administratorzy mogą realizować następujące zadania: • Ochrona komputera jeszcze przed uruchomieniem systemu Windows® • Ochrona konta systemu Windows za pomocą silnego uwierzytelnienia • Zarządzanie danymi logowania i hasłami do stron internetowych i aplikacji • Przeprowadzenie łatwej zmiany hasła systemu operacyjnego Windows • Wykorzystanie czytnika linii papilarnych dla zapewnienia dodatkowego bezpieczeństwa i wygody • Konfiguracja karty inteligentnej, bezstykowej i zbliżeniowej w celu uwierzytelniania • Wykorzystanie telefonu z funkcją Bluetooth jako metody identyfikacji • Wykorzystanie kodu PIN jako dodatkowej opcji uwierzytelniania • Konfiguracja zasad logowania i zasad sesji • Tworzenie kopii zapasowych danych programowych • Dodawanie innych aplikacji, takich jak HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager oraz HP Computrace Użytkownicy mogą realizować następujące zadania: • Przeglądanie ustawień stanu szyfrowania i programu Device Access Manager. • Aktywacja usługi Computrace. • Konfiguracja ustawień oraz tworzenie kopii zapasowych i przywracania.
Dostęp do programu Password Manager	Użytkownicy mogą realizować następujące zadania: • Tworzenie i porządkowanie nazw użytkownika i haseł. • Tworzenie silniejszych haseł w celu zwiększenie bezpieczeństwa skrzynki poczty elektronicznej i kont internetowych. Password Manager wstawia i udostępnia niezbędne informacje w sposób automatyczny. • Uproszczenie procesu logowania dzięki funkcji Single Sign On, umożliwiające automatyczne zapisywanie i wstawianie danych uwierzytelniających użytkownika. • Oznaczenie danego konta jako zagrożonego włamaniem po to, by aktywować ostrzeżenia dla innych kont, do których dostęp jest zabezpieczony za pomocą podobnych danych uwierzytelniających. • Importowanie danych logowania z pamięci przeglądarki.

Moduł	Funkcje kluczowe
HP Drive Encryption (tylko wybrane modele)	• Umożliwia szyfrowanie całych woluminów dysku. • Wymusza uwierzytelnianie przedrozruchowe w celu deszyfracji i umożliwienia dostępu do danych. • Umożliwia aktywację opcji autoszyfrowania dysków (tylko wybrane modele).
HP Device Access Manager	• Umożliwia nadzór nad dostępem do urządzeń poprzez profile użytkownika. • Uniemożliwia osobom nieuprawnionym przenoszenia danych na zewnętrzne urządzenia pamięci masowej oraz niweluje ryzyko zainfekowania systemu przez wirusy przenoszone przez te urządzenia. • Pozwala administratorom na blokowanie dostępu do urządzeń wymiany danych dla indywidualnych użytkowników lub grup użytkowników.
HP Trust Circle	• Zapewnia bezpieczeństwo plików i dokumentów. • Szyfruje pliki w określonym przez użytkownika folderze i chroni je wewnątrz zdefiniowanego kręgu zaufania. • Umożliwia udostępnianie i wykorzystywanie plików jedynie przez osoby z danego kręgu zaufania.
Odzyskiwanie urządzenia w przypadku kradzieży (Nabywany oddzielnie dostęp do usługi Computrace)	• W celu aktywacji oprogramowania umożliwiającego namierzenie skradzionego urządzenia niezbędne jest wykupienie subskrypcji. • Umożliwia bezpieczne śledzenie zasobów. • Monitoruje aktywność użytkownika oraz zmiany dokonywane w sprzęcie i oprogramowaniu. • Program pozostaje aktywny nawet w przypadku sformatowania lub wymiany dysku.

HP Client Security – opis produktu i przykłady wykorzystania

Większość programów pakietu HP Client Security posiada możliwość wykonania kopii zapasowej danych uwierzytelniających (zwykle hasła) oraz kopii zapasowej administratora, umożliwiających uzyskanie dostępu w przypadku, gdy hasła zostały zagubione, zapomniane lub z innych powodów nie są dostępne. Umożliwiają one również uzyskanie dostępu w przypadkach, gdzie wymaga tego polityka bezpieczeństwa firmy.

UWAGA: Niektóre programy pakietu HP Client Security zostały stworzone w celu ograniczenia dostępu do danych. W przypadku, gdy bardziej korzystna z punktu widzenia firmy jest utrata informacji, niż możliwość ich wykradzenia, dane powinny być szyfrowane. Zaleca się, aby wszystkie kopie zapasowe były przechowywane w bezpiecznym miejscu.

Dostęp do programu Password Manager

Program Password Manager przechowuje nazwy użytkownika i hasła. Może być on wykorzystywany do:

- Zapisywania nazw użytkownika i haseł dla stron internetowych i poczty elektronicznej.
- Automatycznego logowania użytkownika na stronach internetowych lub kontach poczty elektronicznej.
- Zarządzania i porządkowania danych uwierzytelniających.
- Wyboru zasobów internetowych i sieciowych oraz umożliwienia bezpośredniego do nich dostępu poprzez zapisane łącze.
- Wyświetlania nazw i haseł internetowych, gdy jest to konieczne.
- Oznaczenia danego konta jako zagrożonego włamaniem po to, by aktywować ostrzeżenia dla innych kont, do których dostęp jest zabezpieczony za pomocą podobnych danych uwierzytelniających.
- Importowania danych logowania z pamięci przeglądarki.

Przykład 1: Zaopatrzeniowiec w dużej firmie wykonuje większość transakcji drogą internetową. Osoba ta również odwiedza kilka stron internetowych wymagających logowania. Zna ona zasady bezpieczeństwa i wie, że nie powinna ustawiać tych samych danych logowania na wszystkich tych stronach. Zaopatrzeniowiec decyduje się na użycie programu Password Manager, by w prosty sposób logować się na różne strony internetowe za pomocą różnych nazw użytkownika i haseł. Po wejściu na stronę logowania danej witryny internetowej, Password Manager wstawia wszelkie dane uwierzytelniające w sposób automatyczny. Jeśli użytkownik chce przeglądnąć nazwy użytkownika i hasła, Password Manager może zostać skonfigurowany w taki sposób, aby były one wyświetlane.

Password Manager może być również wykorzystywany do zarządzania i porządkowania danych uwierzytelniających. Program ten umożliwia również szybki dostęp do określonych zasobów internetowych i sieciowych poprzez użycie zapisanego łącza. Użytkownik może także wyświetlać nazwy użytkownika i hasła, gdy jest to konieczne.

Przykład 2: Pewien pracownik, dzięki wysokim wynikom otrzymał awans i będzie od teraz kierował całym działem księgowości. Wszyscy zatrudnieni w dziale pracownicy muszą logować na wielu stronach internetowych klientów firmy, na każdą z nich przy użyciu innej nazwy użytkownika i hasła. Te dane uwierzytelniające muszą być współdzielone między wieloma pracownikami, przy jednoczesnym zachowaniu wszelkich zasad bezpieczeństwa i poufności. Pracownik ten, po rozpoczęciu pracy na nowym stanowisku decyduje, że wszelkie łącza, nazwy użytkowników i hasła będą nadzorowane przez program Password Manager. Po wdrożeniu programu Password Manager, pracownicy działu mogą logować się na poszczególnych stronach bez znajomości danych uwierzytelniających.

HP Drive Encryption (tylko wybrane modele)

Program HP Drive Encryption jest wykorzystywane w celu ograniczenia dostępu osób niepowołanych do danych zapisanych na dysku komputera lub dyskach pomocniczych. Drive Encryption obsługuje również dyski samoszyfrujące.

Przykład 1: Lekarz chce mieć pewność, że nikt inny oprócz niego nie uzyska dostępu do danych zapisanych na dysku jego komputera. Aktywuje on program Drive Encryption, który wymaga uwierzytelnienia przedrozruchowego, jeszcze przed zalogowaniem się do systemu Windows. Po wprowadzeniu takich ustawień, dostęp do twardego dysku komputera przed uruchomieniem systemu Windows jest możliwy dopiero po wprowadzeniu hasła. Lekarz ten może również zdecydować się na

dodatkowe zabezpieczenie zgromadzonych na dysku informacji poprzez zastosowanie opcji samoszyfrowania danych.

Przykład 2: Dyrektor szpitala chce mieć pewność, że jedynie lekarze i uprawniony personel uzyskają dostęp do danych na lokalnym komputerze, bez konieczności zaznajamiania tych osób z prywatnymi hasłami dostępu. Informatycy szpitala dodają doktora, lekarzy i inne uprawnione osoby do grona użytkowników Drive Encryption. Od tej chwili jedynie osoby uprawnione są w stanie uruchomić komputer lub wejść na domenę za pomocą swoich prywatnych nazw użytkownika i haseł.

HP Device Access Manager (tylko wybrane modele)

HP Device Manager umożliwia administratorowi blokowanie i zarządzanie dostępem do sprzętu. Device Access Manager może być używany w celu blokowania nieuprawnionego dostępu do przenośnych urządzeń pamięci masowej, umożliwiających kopiowanie danych. Można również ograniczyć dostęp do napędu CD/DVD, urządzeń podpiętych do gniazd USB, połączeń sieciowych itd. Za przykład może posłużyć sytuacja, w której chcemy, by zewnętrzni dostawcy uzyskali dostęp do komputerów firmy, lecz bez możliwości kopiowania danych na przenośne urządzenia pamięci masowej.

Przykład 1: Kierownik firmy dostarczającej materiały medyczne często korzysta z informacji wewnętrznych oraz indywidualnych danych medycznych. Pracownicy potrzebują dostępu do tych danych, jednak dane te pod żadnym pozorem nie mogą być kopiowane na żadne zewnętrzne urządzenia magazynowania danych. Wewnętrzna sieć firmowa jest zabezpieczona, lecz komputery na których dane są przechowywane są wyposażone w nagrywarki CD i gniazda USB, co umożliwia kradzież i kopiowanie danych. Kierownik może wykorzystać program Device Access Manager, by dezaktywować porty USB i napędy CD tak, aby nie mogły być wykorzystane do nielegalnego skopiowania danych. Pomimo blokady portów USB myszy i klawiatury komputerów będą działać.

Przykład 2: Firma ubezpieczeniowa nie życzy sobie, by jej pracownicy instalowali na własna rękę jakiekolwiek oprogramowanie i przechowywali dane prywatne na firmowych komputerach. Niektórzy pracownicy firmy jednak będą potrzebować dostępu do aktywnych portów USB na wszystkich komputerach. Informatyk firmy, poprzez program Device Access Manager umożliwia niektórym pracownikom dostęp do portów USB, blokując jednocześnie dostęp dla pozostałych.

Usługa Computrace (do oddzielnego zakupu)

Computrace (do oddzielnego zakupu) to usługa umożliwiająca ustalenie położenia skradzionego komputera w momencie, gdy urządzenia zostanie podłączone do Internetu. Usługa Computrace pomaga również w zdalnym zarządzaniu i lokalizowaniu komputerów, a także monitorowaniu pracy komputera i użycia poszczególnych aplikacji.

Przykład 1: Dyrektor szkoły prosił dział informatyczny o monitorowanie wszystkich komputerów będących własnością szkoły. Po zinwentaryzowaniu wszystkich urządzeń, administrator IT zarejestrował je w Computrace tak, by mogły zostać namierzone w przypadku kradzieży. Zauważono ostatnio, że w szkole brakuje kilku komputerów. Administrator IT poinformował o tym dyrektora szkoły i dostawcę usługi Computrace. Komputery zostały zlokalizowane i zwrócone do szkoły przez odpowiednie służby.

Przykład 2: Pewna agencja nieruchomości chce aktualizować i zarządzać komputerami w poszczególnych oddziałach rozsianych po całym świecie. Wykorzystują Computrace do monitorowania i aktualizacji komputerów bez konieczności wysyłania informatyka do każdego komputera z osobna.

Osiągnięcie kluczowych celów bezpieczeństwa

Poszczególne moduły oprogramowania HP Client Security mogą działać jednocześnie, rozwiązując wiele kwestii związanych z zabezpieczeniami i realizując następujące cele bezpieczeństwa:

- Ochrona przed zaplanowaną kradzieżą
- Ograniczenie dostępu do danych poufnych
- Uniemożliwienie nieuprawnionego dostępu z lokalizacji wewnętrznych i zewnętrznych
- Tworzenie mocnych haseł

Ochrona przed zaplanowaną kradzieżą

Przykładem zaplanowanej kradzieży może być próba wykradzenia komputera zawierającego informacje poufne i dane osobowe, na przykład komputera zainstalowanego w punkcie kontrolnym na lotnisku. Następujące funkcje oprogramowania pomagają w ochronie przeciwko zaplanowaną kradzieżą:

- Uwierzytelnianie przedrozruchowe. Jeśli opcja ta jest włączona, nieautoryzowany dostęp do systemu operacyjnego jest niemożliwy.
  - HP Client Security — patrz: HP Client Security na stronie 14.
  - HP Drive Encryption — patrz HP Drive Encryption (tylko wybrane modele) na stronie 33.
- Szyfrowanie sprawia, że nieuprawniony dostęp do danych jest niemożliwy, nawet w przypadku, gdy twardy dysk zostanie przełożony do komputera z niezabezpieczonym systemem operacyjnym.
- Usługa Computrace umożliwia zlokalizowanie komputera po kradzieży.
  - Computrace — patrz: Odzyskiwanie sprzętu po kradzieży (tylko wybrane modele) na stronie 58.

Ograniczenie dostępu do danych poufnych

Załóżmy, że audytor projektu pracujący w terenie otrzymał dostęp do poufnych danych finansowych. Nie chcesz jednak, by miał on możliwość drukowania tych danych lub zapisywania ich na jakimkolwiek nośniku, na przykład na dysku CD. Następujące funkcje pomagają ograniczyć dostęp do danych:

- HP Device Manager pozwala administratorom IT na ograniczenie dostępu do urządzeń komunikacyjnych, uniemożliwiając kopiowania poufnych informacji z twardego dysku. Zobacz Widok systemu na stronie 48.

Uniemożliwienie nieuprawnionego dostępu z lokalizacji wewnętrznych i zewnętrznych

Nieuprawniony dostęp do niezabezpieczonego komputera firmowego stanowi wielkie zagrożenie dla danych przechowywanych na wszystkich komputerach sieci wewnętrznej firmy. Z komputerów mogą zostać wykradzione informacje o usługach finansowych, informacje zarządu, dane zespołu ds. badań

i rozwoju lub dane osobowe, jak choćby prywatne dane medyczne lub finansowe. Następujące funkcje pomagają zablokować nieuprawniony dostęp:

- Uwierzytelnianie przedrozruchowe. Jeśli opcja ta jest włączona, nieautoryzowany dostęp do systemu operacyjnego jest niemożliwy. (patrz HP Drive Encryption (tylko wybrane modele) na stronie 33.
- Pakiet HP Client Security pozwala zablokować dostęp osób nieuprawnionych do haseł i aplikacji chronionych hasłami. Zobacz HP Client Security na stronie 14.
- HP Device Manager pozwala informatykom na ograniczenie dostępu do urządzeń zapisu danych, uniemożliwiając kopiowania poufnych informacji z twardego dysku. Zobacz HP Device Access Manager (tylko wybrane modele) na stronie 47.

Tworzenie mocnych haseł

Jeśli polityka firmy wymaga tworzeni mocnych haseł dla kilkudziesięciu aplikacji sieciowych i baz danych wymagających logowania, program Password Manager może być wykorzystywany jako bezpieczny magazyn do ich przechowywania, zapewniając jednocześnie możliwość korzystania z usługi Single Sign On (jednokrotne logowanie). Zobacz Dostęp do programu Password Manager na stronie 20.

Dodatkowe elementy bezpieczeństwa

Przypisywanie ról bezpieczeństwa

W zarządzaniu ochroną komputera (zwłaszcza w przypadku dużych firm) szczególnie ważne jest rozdzielenie praw i odpowiedzialności pomiędzy różne grupy administratorów i użytkowników.

UWAGA: W małej organizacji lub w przypadku indywidualnego użytkowania komputera wszystkie te role mogą być pełnione przez jedną osobę.

W przypadku oprogramowania HP Client Security, wszystkie obowiązki i przywileje dotyczące bezpieczeństwa mogą zostać rozdzielone między osoby pełniące następujące role:

- Funkcjonariusz ds. bezpieczeństwa – Określa poziom bezpieczeństwa firmy lub sieci i określa rodzaje zabezpieczeń które należy wdrożyć, na przykład zastosowanie programu Drive Encryption.

  UWAGA: Wiele funkcji programów tworzących pakiet HP Client Security może być zmienianych przez funkcjonariusza ds. bezpieczeństwa we współpracy z HP. Więcej informacji można znaleźć w rozdziale http://www.hp.com.

- Administrator IT – Wprowadza i zarządza zabezpieczeniami zdefiniowany przez funkcjonariusza ds. bezpieczeństwa. Może również aktywować i dezaktywować niektóre funkcje bezpieczeństwa. Na przykład, jeśli funkcjonariusz ds. bezpieczeństwa zdecyduje się na wprowadzenie kart inteligentnych, administrator IT może aktywować uwierzytelnianie zarówno za pomocą hasła, jak i kart inteligentnych.
- Użytkownik – Wykorzystuje aktywowane funkcje bezpieczeństwa. Na przykład, jeśli funkcjonariusza ds. bezpieczeństwa i administrator IT aktywowali tryb uwierzytelniania za pomocą kart inteligentnych dla systemu, użytkownik może ustalić numer PIN karty i korzystać z karty podczas uwierzytelniania.

OSTROŻNIE: Zachęca się administratorów IT do stosowania najlepszych praktyk bezpieczeństwa ograniczających przywileje użytkownika końcowego i wprowadzania ograniczeń dostępu.

Użytkownicy niepowołani nie powinni otrzymywać przywilejów administracyjnych.

Zarządzanie hasłami w pakiecie HP Client Security

Większość funkcji bezpieczeństwa pakietu HP Client Security jest chroniona za pomocą haseł. Poniższa tabela zawiera listę powszechnie używanych haseł, moduły pakietu HP Client Security w których są one wykorzystywane oraz funkcje haseł.

Hasła ustanawiane i używane jedynie przez administratorów IT zostały również wyszczególnione w tabeli. Wszystkie inne hasła mogą być ustanawiane i używane przez zwykłych użytkowników lub administratorów.

Hasło oprogramowania HP Client Security	Ustanowione w następującym module	Funkcja
hasło logowania do systemu Windows	Panelu sterowania systemu Windows lub HP Client Security	Można go używać do ręcznego logowania oraz uwierzytelniania w celu uzyskania dostępu do różnych funkcji pakietu HP Client Security.
hasło do HP Client Security Backup and Recovery	HP Client Security, ustanawiane przez użytkownika	Zabezpiecza dostęp do HP Client Security Backup i pliku odzyskiwania.
PIN karty inteligentnej	Credential Manager	Może być wykorzystywany jako uwierzytelnianie wieloczynnikowe. Może być wykorzystywany jako uwierzytelnianie podczas logowania do systemu Windows. Uwierzytelnia użytkowników Drive Encryption, jeśli został wybrany tryb karty inteligentnej.

Tworzenie bezpiecznego hasła

Podczas tworzenia hasła, należy przestrzegać wszelkich wymogów narzuconych przez program. Na ogół należy stosować się do następujących wskazówek, by móc utworzyć mocne hasło i zminimalizować ryzyko jego złamania:

- Hasło powinno składać się z co najmniej 6 znaków, zaleca się jednak, by składało się z ponad 8 znaków.
- Podczas tworzenia hasła wymieszaj małe litery z wielkimi.
- Zawsze, gdy jest to możliwe, łącz litery z cyframi, dodając znaki specjalne i interpunkcyjne.
- W słowie kluczowym wstaw znaki specjalne lub cyfry zamiast niektórych liter. Na przykład, w miejsce I lub L wstaw cyfrę 1.
- Łącz słowa pochodzące z dwóch lub kilku języków.
- Rozdzielaj wyrazy lub frazy za pomocą cyfr lub znaków specjalnych, na przykład "Mary2-2Cat45."
- nie używaj haseł, które występują w słowniku.
- Nie używaj imion, nazwisk lub jakichkolwiek innych informacji prywatnych, takich jak data urodzin, imiona zwierząt domowych, nazwisk panieńskich, nawet pisanych wspak.
- Regularnie zmieniaj hasła. Wystarczy zmian tylko kilku znaków w haśle.
- Jeśli zapisujesz hasło na kartce, nie trzymaj go w widocznym miejscu w okolicy komputera.

- Nie należy zapisywać hasła na komputerze w pliku lub jako zawartości listy e-mailowego.
- Nie udostępniaj konta i nikomu nie zdradzaj hasła.

Tworzenie kopii zapasowej danych uwierzytelniających i ustawień

Jako centralnej lokalizacji, z poziomu której można tworzyć kopie zapasowe i odzyskiwać dane uwierzytelniające dla niektórych z zainstalowanych modułów pakietu HP Client Security można użyć narzędzia Backup and Recovery, stanowiącego również część pakietu HP Client Security.

2 Rozpoczęcie pracy

By oprogramowanie HP Client Security mogło wykorzystywać twoje dane uwierzytelniające, uruchom aplikację HP Client Security w jeden z następujących sposobów. Po zakończeniu pracy kreatora konfiguracji nie może być on ponownie uruchomiony przez użytkownika.

1. Na ekranie głównym lub ekranie aplikacji kliknij lub naciśnij ikonę aplikacji **HP Client Security** (Windows 8).

   — lub —

   Na pulpicie systemu Windows kliknij lub naciśnij ikonę aplikacji **HP Client Security Gadget** (Windows 7).

   — lub —

   Na pulpicie systemu Windows dwukrotnie kliknij lub naciśnij ikonę **HP Client Security** umieszczoną w obszarze powiadomień, z prawej strony paska zadań.

   — lub —

   Na pulpicie systemu Windows dwukrotnie kliknij lub naciśnij ikonę **HP Client Security** umieszczoną w obszarze powiadomień, a następnie wybierz **Open HP Client Security** (Otwórz aplikację HP Client Security).

2. Kreator konfiguracji aplikacji HP Client Security zostanie uruchomiony wraz z ekranem powitalnym.

3. Przeczytaj zawartość ekranu powitalnego, a następnie potwierdź swoją tożsamość poprzez wprowadzenie hasła dostępu do systemu Windows, po czym kliknij lub naciśnij **Next** (Dalej).

   Jeśli hasło Windows nie zostało jeszcze ustawione, zostanie wyświetlony monit o utworzenie hasła. Ustanowienie hasła dostępu do Windows jest niezbędne, aby chronić konto Windows przed dostępem osób nieupoważnionych, oraz, aby móc wykorzystać wszystkie dostępne możliwości programu HP Client Security.

4. Na stronie HP SpareKey wybierz trzy pytania bezpieczeństwa. Wprowadź odpowiedź na każde z pytań, a potem kliknij **Next** (Dalej). Dopuszcza się wprowadzenie pytań niestandardowych. Aby uzyskać więcej informacji, zobacz HP SpareKey — Odzyskiwanie hasła na stronie 16.

5. Na stronie Fingerprints (Linie papilarne) zarejestruj minimalną lub większą od minimalnej ilość odcisków palców, a potem kliknij lub naciśnij **Next** (Dalej). Aby uzyskać więcej informacji, zobacz Linie papilarne na stronie 15.

6. Na stronie Drive Encryption (Szyfrowanie dysków) aktywuj szyfrowanie, utwórz kopię zapasową klucza szyfrującego, a następnie kliknij lub naciśnij **Next** (Dalej). Dodatkowe informacje zamieszczono w pliku pomocy programu HP Drive Encryption.

UWAGA: Dotyczy to sytuacji, gdy użytkownik jest jednocześnie administratorem, a program HP Client Security nie został wcześniej skonfigurowany przez administratora.

7. Na ostatniej stronie kreatora konfiguracji kliknij lub naciśnij **Finish** (Zakończ).

   Strona ta prezentuje status funkcji i danych uwierzytelniających.

8. Kreator konfiguracji HP Client Security zapewnia aktywację funkcji uwierzytelnienia Just In Time Authentication oraz funkcji programu File Sanitizer. Dodatkowe informacje zamieszczono w dokumentach pomocy programów HP Device Access Manager oraz HP File Sanitizer.

UWAGA: Dotyczy to sytuacji, gdy użytkownik jest jednocześnie administratorem, a program HP Client Security nie został wcześniej skonfigurowany przez administratora.

Uruchamianie programu HP Client Security

Program HP Client Security można uruchomić w jeden z poniższych sposobów:

UWAGA: Przed uruchomieniem programu HP Client Security, kreator konfiguracji HP Client Security Setup Wizard musi zakończyć swoją pracę.

- Na ekranie głównym lub ekranie aplikacji kliknij lub naciśnij ikonę **HP Client Security**.

  — lub —

  Na pulpicie systemu Windows kliknij lub naciśnij ikonę aplikacji **HP Client Security Gadget** (Windows 7).

  — lub —

  Na pulpicie systemu Windows dwukrotnie kliknij lub naciśnij ikonę **HP Client Security** umieszczoną w obszarze powiadomień, z prawej strony paska zadań.

  — lub —

  Na pulpicie systemu Windows dwukrotnie kliknij lub naciśnij ikonę **HP Client Security** umieszczoną w obszarze powiadomień, a następnie wybierz **Open HP Client Security** (Otwórz aplikację HP Client Security).

3 Instrukcja prostej instalacji dla małych firm

Rozdział ten zawiera najprostsze sposoby aktywacji najczęściej stosowanych i najbardziej użytecznych funkcji i opcji pakietu oprogramowania HP Client Security dla małych firm. Liczne narzędzia i opcje pakietu pozwalają na odpowiednie ustawienie preferencji i kontroli dostępu. Głównym celem utworzenia tego uproszczonego przewodnika było umożliwienie użytkownikowi uruchomienie poszczególnych modułów bez nadmiernego wysiłku i w krótkim czasie. Aby uzyskać dodatkowe informacje wybierz moduł który Cię interesuje, a następnie kliknij **?** lub przycisk Pomoc w prawym górnym rogu. Przycisk ten umożliwia automatyczne wyświetlenie informacji związanych z bieżąco wyświetlanym oknem.

Rozpoczęcie pracy

1. Na pulpicie Windows otwórz HP Client Security, klikając dwukrotnie ikonę **HP Client Security** w obszarze powiadomień znajdującym się z prawej strony paska zadań.
2. Wprowadź hasło systemu Windows, lub utwórz hasło systemu.
3. Zakończenie konfiguracji oprogramowania HP Client Security.

Aby program HP Client Security żądał uwierzytelniania tylko raz podczas logowania do systemu Windows, patrz: Opcje zabezpieczeń na stronie 29

Dostęp do programu Password Manager

Każdy z nas korzysta ze sporej ilości haseł, zwłaszcza jeśli regularnie odwiedza strony internetowe i używa aplikacji wymagających logowania. Przeciętny użytkownik zwykle korzysta z tego samego hasła do wszystkich stron i aplikacja lub wykazuje się kreatywnością i do każdej strony i aplikacji tworzy nowe hasło. Niestety, to drugie rozwiązanie często skutkuje zapomnieniem poszczególnych haseł.

Program Password Manager jest w stanie w sposób automatyczny zapamiętać hasła do poszczególnych stron i aplikacji lub umożliwi rozpoznanie stron do których hasła należy zapamiętać, a dla których nie jest to konieczne. Po zalogowaniu do komputera, Password Manager samodzielnie odszuka w pamięci hasła lub dane uwierzytelniające poszczególnych aplikacji lub stron internetowych.

Po wejściu na stronę wymagająca logowania, program Password Manager w sposób automatyczny rozpozna stronę i wygeneruje komunikat z zapytaniem, czy chcesz, aby dane logowania zostały zapamiętane. Jeśli chcesz, aby pewne strony internetowe nie zostały objęte tą procedurą możesz odmówić.

Aby rozpocząć zapisywanie danych stron, nazw użytkownika i haseł:

1. Przejdź do przykładowej strony internetowej lub aplikacji, a następnie kliknij ikonę Password Manager w górnym lewym rogu strony internetowej. Dane uwierzytelniające dla strony zostaną zapisane.
2. Wprowadź do programu Password Manager nazwę łącza (opcjonalnie), nazwę użytkownika i hasło.

3. Po zakończeniu kliknij przycisk **OK**.
4. Menedżer Haseł można również zapisać nazwę użytkownika i hasła do aplikacji udostępnianych w sieci lub mapowanych dysków sieciowych.

Wyświetlanie i zarządzanie zapisanymi w programie Password Manager danymi uwierzytelniającymi.

Menedżer Haseł umożliwia wyświetlanie, zarządzanie archiwizację i wprowadzanie danych uwierzytelniających z centralnej lokalizacji. Password Manager obsługuje również otwieranie zapisanych stron z poziomu Windows.

Aby otworzyć program Password Manager, użyj kombinacji klawiszy Ctrl+Windows key+h, a następnie kliknij **Log in** by uruchomić zapisany skrót i przeprowadzić logowanie.

Opcja **Edytuj** w programie Password Manager umożliwia wyświetlanie i modyfikowanie nazwy, nazwy używanej do logowania, a nawet hasła.

HP Client Security dla małych firm umożliwia wykonanie kopi zapasowej lub/oraz skopiowanie danych uwierzytelniających i ustawień na inny komputer.

HP Device Access Manager

Manager może być wykorzystywany do zablokowania możliwości użycia jakichkolwiek wewnętrznych lub zewnętrznych urządzeń przechowywania danych tak, by dane na twardym dysku były zabezpieczone przed nieuprawnionym skopiowaniem i nie "wyciekły" z twojej firmy. Program umożliwia udostępnienie dowolnemu użytkownikowi danych zgromadzonych na twoim komputerze, lecz blokuje jakiekolwiek próby ich kopiowania na dyski CD, odtwarzacze muzyki wyposażone w pamięć, przenośne urządzania pamięci masowej lub inne urządzenia przechowywania danych.

1. Otwórz **Device Access Manager** (patrz: Uruchamianie programu Device Access Manager na stronie 47)

   Wyświetli się dostęp dla bieżącego użytkownika.
2. Aby zmienić dostęp dla użytkowników, grup użytkowników lub urządzeń, kliknij lub naciśnij **Zmień**. Aby uzyskać więcej informacji, zobacz Widok systemu na stronie 48.

HP Drive Encryption

Program HP Drive Encryption jest używane do ochrony danych poprzez szyfrowanie całego twardego dysku. Dane zapisane na twardym dysku twojego komputera pozostaną bezpieczne nawet w przypadku jego kradzieży i/lub próby przełożenia twardego dysku do innego komputera.

Dodatkową korzyść stanowi fakt, że program Drive Encryption wymaga uwierzytelnienia za pomocą nazwy użytkownika i hasła jeszcze przed uruchomieniem systemu operacyjnego. Proces ten nosi nazwę uwierzytelniania przedrozruchowego.

Aby ułatwić użytkowanie komputera, poszczególne moduły pakietu synchronizują hasła w sposób automatyczny, w tym hasła do systemu Windows, dane uwierzytelniające domen, HP Drive Encryption, Password Manager i HP Client Security.

Aby odpowiednio ustawić parametry programu HP Drive Encryption podczas początkowej konfiguracji za pomocą kreatora konfiguracji HP Client Security, patrz: Rozpoczęcie pracy na stronie 10.

4 HP Client Security

Strona główna HP Client Security Home to lokalizacja, z poziomu której można w łatwy sposób uzyskać dostęp do funkcji, aplikacji oraz ustawień programu HP Client Security. Strona główna programu jest podzielona na trzy sekcje:

- **DATA** (DANE) — Umożliwia dostęp do aplikacji wykorzystywanych do zarządzania bezpieczeństwem danych.
- **DEVICE** (URZĄDZENIE) — Umożliwia dostęp do aplikacji używanych do zarządzania bezpieczeństwem urządzeń.
- **IDENTITY** (TOŻSAMOŚĆ) — Umożliwia rejestrowanie danych i urządzeń uwierzytelniających oraz zarządzanie nimi.

Przesuń kursor na kafelek aplikacji, aby obejrzeć jej opis.

Program HP Client Security może udostępnić dodatkowe łącza do ustawień użytkownika i administratora w dolnej części strony. Program HP Client Security zapewnia dostęp do Ustawień zaawansowanych i funkcji poprzez kliknięcie lub naciśnięcie ikony **Gear** (Ustawienia).

Aplikacje, funkcje i ustawienia tożsamości

Aplikacje, funkcje i ustawienia tożsamości w programie HP Client Security pomagają w zarządzaniu wieloma aspektami twojej cyfrowej tożsamości. Klikaj lub naciskaj jeden z poniższych kafelków na stronie głównej programu HP Client Security, a następnie wprowadź hasło dostępu do systemu Windows:

- **Fingerprints** (Linie papilarne) — Rejestruje i zarządza danymi związanymi z uwierzytelnianiem za pomocą linii papilarnych.
- **SpareKey** (Klucz zapasowy) — Tworzy i zarządza danymi uwierzytelniającymi z kluczy zapasowych HP SpareKey, które mogą być wykorzystywane do logowania na komputerze w przypadku utraty lub zagubienia pozostałych danych uwierzytelniających. Funkcja ta pozwala także na zresetowanie zapomnianego hasła.
- **Windows Password** (Hasło dostępu do systemu Windows) — Umożliwia łatwą zmianę hasła dostępu do systemu Windows.
- **Bluetooth Devices** (Urządzenia Bluetooth) — Umożliwia rejestrację i zarządzanie urządzeniami Bluetooth.
- **Cards** (Karty) — Umożliwia rejestrację i zarządzanie kartami inteligentnymi, bezstykowymi i zbliżeniowymi.
- **PIN** (Kod PIN) — Umożliwia rejestrację i zarządzanie kodami PIN.
- **RSA SecurID** — Pozwala na rejestrację i zarządzanie danymi uwierzytelniającymi RSA SecurID (jeśli odpowiednia konfiguracja jest dostępna).
- **Password Manager** (Manager haseł) — Umożliwia zarządzanie hasłami do kont sieciowych i aplikacji.

Linie papilarne

Kreator konfiguracji programu HP Client Security Setup poprowadzi cię przez proces konfiguracji lub „rejestracji” twoich linii papilarnych.

Możesz również rejestrować lub usuwać linie papilarne na stronie Fingerprints (Linie papilarne). Aby wejść na stronę, należy kliknąć lub nacisnąć ikonę **Fingerprints** (Linie papilarne), znajdującą się na stronie startowej programu HP Client Security.

1. Będąc na stronie Linie papilarne przyłóż wybrany palec do czytnika linii papilarnych, aż zostanie zarejestrowany.

   Minimalna liczba palców do zarejestrowania została wskazana na stronie. Zaleca się rejestrację palca środkowego lub wskazującego.

2. Aby usunąć wcześniej zarejestrowane odciski palców, kliknij lub naciśnij **Delete** (Usuń).

3. Aby zarejestrować dodatkowe palce, kliknij lub naciśnij **Enroll an additional fingerprint** (Zarejestruj dodatkowy palec).

4. Przed opuszczeniem strony kliknij lub naciśnij **Save** (Zapisz).

⚠ **OSTROŻNIE:** W przypadku rejestracji linii papilarnych w kreatorze, informacje na ich temat zostaną zapisane dopiero po naciśnięciu przycisku **Next** (Dalej). W przypadku pozostawienia komputera nieaktywnego przez pewien czas lub w przypadku zamknięcia programu, wprowadzone zmiany **nie** zostaną zapisane.

- ▲ Aby uzyskać dostęp do ustawień administracyjnych linii papilarnych, gdzie administratorzy mogą definiować rejestrację, dokładność czytnika i inne ustawienia, kliknij lub naciśnij **Administrative Settings** (Ustawienia Administracyjne) — (wymaga uprawnień administratora).
- ▲ Aby uzyskać dostęp do ustawień użytkownika linii papilarnych, gdzie użytkownicy mogą zarządzać widokami i zachowaniami funkcji rozpoznawania linii papilarnych, kliknij lub naciśnij **User Settings** (Ustawienia użytkownika).

Ustawienia administracyjne linii papilarnych

Administratorzy mogą określać parametry dotyczące rejestracji, dokładności czytnika i inne ustawienia dotyczące czytnika linii papilarnych. Do wprowadzania zmian są konieczne uprawnienia administratora.

- ▲ Aby uzyskać dostęp do ustawień administracyjnych linii papilarnych, kliknij lub naciśnij **Administrative Settings** (Ustawienia administracyjne) na stronie Linie papilarne.
- **User enrollment** (Rejestracja użytkownika) — Wybierz minimalną i maksymalną liczbę palców, która może być zarejestrowana przez użytkownika.
- **Recognition** (Rozpoznawanie) — Przesuń suwak w celu dostosowania czułości czytnika podczas sczytywania linii papilarnych.

  Jeśli twoje linie papilarne nie są rozpoznawane, należy obniżyć ustawienia czułości rozpoznawania. Wyższe ustawienia zwiększają czułość czytnika, zmniejszając prawdopodobieństwo omyłkowej akceptacji niezarejestrowanych odcisków palców. Ustawienie **Medium-High** (Średnie-wysokie) zapewnia zarówno niezbędną ochronę, jak i wygodę dla użytkownika.

Ustawienia użytkownika linii papilarnych

Na stronie Ustawienia użytkownika linii papilarnych można wybrać ustawienia dotyczące widoku i zachowań funkcji rozpoznawania linii papilarnych.

▲ Aby uzyskać dostęp do ustawień użytkownika linii papilarnych, kliknij lub naciśnij **Administrative Settings** (Ustawienia administracyjne) na stronie Linie papilarne.

- **Enable sound feedback** (Aktywuj sygnał dźwiękowy) — Domyślnie program HP Client Security generuje sygnał dźwiękowy podczas sczytywania linii papilarnych, emitując różne dźwięki dla różnych zdarzeń. Możesz przypisać nowe dźwięki do poszczególnych zdarzeń na karcie Dźwięki w ustawieniach dźwięków w panelu sterowania systemu Windows. Odznacz to pole wyboru, aby dezaktywować generowanie dźwięków.
- **Show scan quality feedback** (Pokaż informacje zwrotną skanowania) — Zaznacz to pole wyboru, aby wyświetlić wszystkie wyniki skanowania, niezależnie od jakości. Odznacz to pole, aby wyświetlić jedynie wyniki skanowania dobrej jakości.

HP SpareKey — Odzyskiwanie hasła

Opcja HP SpareKey pozwala na dostęp do komputera po odpowiedzi na trzy pytania bezpieczeństwa (tylko w przypadku komputerów obsługujących tę funkcję).

Program HP Client Security poprosi o skonfigurowanie opcji HP SpareKey podczas wstępnej konfiguracji w kreatorze konfiguracji HP Client Security.

Aby skonfigurować opcję HP SpareKey:

1. Na stronie HP SpareKey kreatora konfiguracji wybierz trzy pytania bezpieczeństwa, a następnie wpisz odpowiedź na każde z nich.

   Można wybrać pytania z dostępnej listy lub zdefiniować własne pytania.

2. Kliknij lub naciśnij **Enroll** (Zarejestruj).

Aby usunąć opcję HP SpareKey:

▲ Kliknij lub naciśnij **Delete your SpareKey** (Usuń klucz zapasowy).

Po skonfigurowaniu usługi SpareKey, istnieje możliwość uzyskania dostępu do komputera przy użyciu opcji z poziomu ekranu logowania przedrozruchowego lub z poziomu ekranu powitalnego systemu Windows.

Można wybierać różne pytania lub zmieniać treść odpowiedzi na stronie SpareKey page, która jest dostępna po kliknięciu kafelka Odzyskiwanie hasła na stronie głównej programu HP Client Security.

Aby uzyskać dostęp do ustawień HP SpareKey, gdzie administrator może definiować ustawienia związane z uwierzytelnieniem za pomocą HP SpareKey, kliknij **Settings** (Ustawienia) (wymagane uprawnienia administratora).

HP SpareKey Settings

Na stronie ustawień HP SpareKey można zdefiniować ustawienia dotyczące zachowań i korzystania z uwierzytelnienia poprzez HP SpareKey.

▲ Aby uruchomić stronę ustawień HP SpareKey, kliknij lub naciśnij **Settings** (Ustawienia) na stronie HP SpareKey (wymaga uprawnień administratora).

Administrator może wybrać następujące ustawienia:

- Określenie pytań, które będą przedstawiane każdemu użytkownikowi podczas konfiguracji HP SpareKey.
- Dodanie trzech własnych pytań do listy pytań prezentowanych użytkownikowi.
- Określenie, czy użytkownik będzie mógł zdefiniować własne pytania.
- Określenie, w jakim środowisku uwierzytelniania (ekran systemu Windows czy ekran przedrozruchowy) ma być uruchamiany HP SpareKey do odzyskania hasła.

hasło systemu Windows

HP Client Security umożliwia szybszą i łatwiejszą zmianę hasła dostępu do systemu Windows niż z poziomu panelu sterowania systemu Windows.

Aby zmienić hasło systemu Windows:

1. Na stronie głównej programu HP Client Security kliknij lub naciśnij **Windows Password** (Hasło systemu Windows).
2. Wprowadź swoje aktualne hasło w polu **Current Windows password** (Aktualne hasło systemu Windows).
3. Wpisz nowe hasło w polu **New Windows password** (Nowe hasło systemu Windows), a następnie wprowadź je ponownie w polu **Confirm new password** (Potwierdź nowe hasło).
4. Kliknij lub naciśnij **Change** (Zmień), aby natychmiast zmienić hasło na nowo wprowadzone.

Urządzenia Bluetooth

Jeśli administrator aktywował łącze Bluetooth jako narzędzie do wprowadzania danych uwierzytelniających, istnieje możliwość skonfigurowania telefonu z funkcją Bluetooth jako dodatkowej metody uwierzytelniania wraz z innymi metodami w celu zwiększenia bezpieczeństwa.

UWAGA: System obsługuje wyłącznie telefony z funkcją Bluetooth.

1. Należy upewnić się, że w komputerze została włączona funkcja Bluetooth, a w telefonie z funkcją Bluetooth jest włączony tryb wykrywania. Ustanowienie połączenia z telefonem może wymagać wprowadzenia automatycznie wygenerowanego kodu w urządzeniu Bluetooth. W zależności od konfiguracji ustawień urządzenia Bluetooth, może być konieczne porównanie kodów parowania pomiędzy komputerem a telefonem.
2. Aby zarejestrować telefon, wybierz go, a następnie kliknij lub naciśnij **Enroll** (Zarejestruj).

Aby uzyskać dostęp do strony Ustawienia urządzeń Bluetooth na stronie 17, na której administrator może wprowadzić ustawienia urządzeń Bluetooth, kliknij **Settings** (Ustawienia)(wymaga uprawnień administratora).

Ustawienia urządzeń Bluetooth

Administratorzy mogą określać poniższe ustawienia, które decydują o zachowaniu i użyciu danych uwierzytelniających urządzeń Bluetooth:

Ciche uwierzytelnienie

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity** (Podczas weryfikacji tożsamości użyj zarejestrowanego urządzenia Bluetooth w sposób automatyczny) — Zaznacz to pole wyboru jeśli chcesz, aby dane uwierzytelniające

użytkowników były przesyłane za pomocą funkcji Bluetooth bez dodatkowych działań użytkownika, lub odznacz pole, aby wyłączyć tę opcję.

Urządzenia Bluetooth w zasięgu

- **Blokuj komputer, gdy zarejestrowane urządzenie Bluetooth znajdzie się poza zasięgiem twojego komputera** — Zaznacz to pole wyboru jeśli chcesz, aby komputer był blokowany, gdy urządzenie Bluetooth, które znajdowało się w zasięgu komputera podczas logowania nagle znajdzie się poza jego zasięgiem lub odznacz, jeśli chcesz, aby opcja ta była nieaktywna.

UWAGA: Moduł Bluetooth zainstalowany w komputerze musi obsługiwać tę funkcję.

Karty

Program HP Client Security obsługuje wiele odmian kart identyfikacyjnych. Są to plastikowe kart z wbudowanym układem scalonym. Do tej grupy należą między innymi karty inteligentne, bezstykowe i zbliżeniowe. Jeśli czytnik karty jest podłączony do komputera, a karta włożona do czytnika oraz jeśli administrator zainstalował odpowiednie sterowniki dostarczone przez producenta, po czym aktywował kartę jako urządzenie uwierzytelniające, to karta ta może być używana do celów uwierzytelniania.

W przypadku kart inteligentnych producent powinien dostarczyć narzędzia umożliwiające zainstalowanie certyfikatu bezpieczeństwa i zarządzanie kodem PIN w taki sposób, aby program HP Client Security mógł go używać do tworzenia algorytmów zabezpieczeń. Liczba i rodzaj znaków w kodzie PIN może się różnić. Przed użyciem karty inteligentnej administrator powinien ją zainicjować.

Program HP Client Security obsługuje następujące formaty kart inteligentnych:

- CSP
- PKCS11

Program HP Client Security obsługuje następujące formaty kart bezstykowych:

- Bezstykowe karty pamięci HID iCLASS
- Bezstykowe karty pamięci MiFare Classic 1k, 4k, i mini karty pamięci

Program HP Client Security obsługuje następujące formaty kart zbliżeniowych:

- Karty zbliżeniowe HID Proximity Cards

Aby zainstalować kartę inteligentną:

1. Włóż kartę do podłączonego czytnika kart inteligentnych.
2. Gdy karta zostanie rozpoznana, wpisz kod PIN, a następnie kliknij lub naciśnij **Enroll** (Zarejestruj).

Aby zmienić kod PIN karty inteligentnej:

1. Włóż kartę do podłączonego czytnika kart inteligentnych.
2. Gdy karta zostanie rozpoznana, wpisz kod PIN, a następnie kliknij lub naciśnij **Authenticate** (Uwierzytelnij).
3. Kliknij lub naciśnij **Change PIN** (Zmień kod PIN), a następnie wprowadź nowy kod PIN.

Aby zarejestrować kartę bezstykową lub zbliżeniową:

1. Połóż kartę na czytniku lub w jego okolicy.
2. Gdy karta zostanie rozpoznana, kliknij lub naciśnij **Enroll** (Zarejestruj).

Aby usunąć zarejestrowana kartę:

1. Przyłóż kartę do czytnika.
2. W przypadku kart inteligentnych wprowadź kod PIN, następnie kliknij lub naciśnij **Authenticate** (Uwierzytelnij).
3. Kliknij lub naciśnij **Delete** (Usuń).

Po zarejestrowaniu karty wszelkie dane na jej temat są wyświetlane w obszarze **Enrolled Cards** (Zarejestrowane karty). Usunięta karta zostanie również usunięta z listy zarejestrowanych kart.

Aby uzyskać dostęp do ustawień kart zbliżeniowych, bezstykowych i inteligentnych, gdzie administratorzy mogą definiować ustawienia związane z uwierzytelnieniami za pomocą tych kart, kliknij lub naciśnij **Settings** (Ustawienia) (wymaga uprawnień administratora).

Ustawienia kart zbliżeniowych, bezstykowych i inteligentnych

Aby uzyskać dostęp do ustawień karty, kliknij lub naciśnij wybraną kartę z listy, a następnie kliknij lub naciśnij strzałkę, która się pojawi.

Aby zmienić kod PIN karty inteligentnej:

1. Przyłóż kartę do czytnika.
2. Wprowadź przypisany do karty kod PIN, a następnie kliknij lub naciśnij **Continue** (Kontynuuj).
3. Wprowadź i potwierdź nowy kod PIN, a następnie kliknij lub naciśnij **Continue** (Kontynuuj).

Aby zainicjować kod PIN karty inteligentnej:

1. Przyłóż kartę do czytnika.
2. Wprowadź przypisany do karty kod PIN, a następnie kliknij lub naciśnij **Continue** (Kontynuuj).
3. Wprowadź i potwierdź nowy kod PIN, a następnie kliknij lub naciśnij **Continue** (Kontynuuj).
4. Kliknij lub naciśnij **Yes** (Tak), aby potwierdzić inicjalizację karty.

Aby usunąć dane z karty:

1. Przyłóż kartę do czytnika.
2. Wprowadź przypisany do karty kod PIN (tylko dla kart inteligentnych), a następnie kliknij lub naciśnij **Continue** (Kontynuuj).
3. Kliknij lub naciśnij **Yes** (Tak), aby potwierdzić usunięcie karty.

PIN

Jeśli administrator aktywował kod PIN jako narzędzie do uwierzytelniania danych, istnieje możliwość ustawienia kodu PIN jako dodatkowej metody uwierzytelniania wraz z innymi metodami w celu zwiększenia bezpieczeństwa.

Aby skonfigurować nowy kod PIN:

- Wprowadź kod PIN, wprowadź go ponownie, a następnie kliknij lub naciśnij **Apply** (Zastosuj).

Aby usunąć kod PIN:

- Kliknij lub naciśnij **Delete** (Usuń), a następnie kliknij lub naciśnij **Yes** (Tak), aby potwierdzić.

Aby uzyskać dostęp do ustawień kodu PIN, gdzie administratorzy mogą definiować ustawienia związane z uwierzytelnieniami za pomocą kodu PIN, kliknij lub naciśnij **Settings** (Ustawienia) (wymaga uprawnień administratora).

PIN Settings (Ustawienia systemu BIOS)

Na stronie ustawień kodu PIN można zdefiniować minimalną i maksymalną długość kodu PIN wykorzystywanego jako uwierzytelnienie.

RSA SecurID

Jeśli administrator aktywował łącze RSA jako narzędzie do uwierzytelniania, a poniższe dane uwierzytelniające są poprawne, możesz rejestrować i usuwać dane uwierzytelniające RSA SecurID.

UWAGA: Wymagana jest odpowiednia konfiguracja.

- Użytkownik musi zostać wcześniej utworzony na serwerze RSA.
- Token RSA SecurID przypisany do użytkownika i komputera musi zostać wcześniej dołączony do domeny serwera RSA.
- Na komputerze jest zainstalowane oprogramowanie SecurID.
- Aby połączenie było dostępne, należy prawidłowo skonfigurować serwer RSA.

Aby zarejestrować uwierzytelnienie RSA SecurID:

▲ Wprowadź nazwę użytkownika i hasło RSA SecurID (kod tokena RSA SecurID lub kod tokena +PIN, w zależności od środowiska), a następnie kliknij lub naciśnij **Apply** (Zastosuj).

Po pomyślnym zakończeniu rejestracji zostanie wyświetlony komunikat „Twoje uwierzytelnienie RSA SecurID zostało pomyślnie zarejestrowane”, a przycisk Usuń zostaje aktywowany.

Aby usunąć uwierzytelnianie RSA SecurID:

▲ Kliknij **Delete** (Usuń), a następnie wybierz **Yes** (Tak), gdy zostanie wyświetlony komunikat o treści „Czy na pewno chcesz usunąć uwierzytelnienie RSA SecurID?”

Dostęp do programu Password Manager

Logowanie do stron internetowych i aplikacji jest łatwiejsze i bezpieczniejsze przy użyciu programu Password Manager. Możesz tworzyć silniejsze hasła i nie musisz ich zapisywać ani zapamiętywać. Możesz zalogować się w prosty sposób przy pomocy linii papilarnych, karty inteligentnej, zbliżeniowej lub bezstykowej, telefonu z funkcją Bluetooth, kodu PIN, uwierzytelniania RSA lub przy użyciu twojego hasła do systemu Windows.

UWAGA: Ze względu na ciągłe zmiany wyglądu ekranów logowania do stron internetowych, program Password Manager może nie być w stanie za każdym razem obsłużyć każdej strony internetowej.

Program Password Manager oferuje następujące opcje:

Strona programu Password Manager

- Kliknij lub naciśnij konto, aby automatycznie otworzyć stronę internetową lub aplikację i zalogować się.
- Przyporządkuj swoja konta do poszczególnych kategorii.

Siła hasła

- Sprawdź, czy któreś z twoich haseł nie jest zbyt słabe i nie zagraża bezpieczeństwu.
- Podczas dodawania danych logowania sprawdź siłę poszczególnych haseł używanych podczas logowania do stronach internetowych i aplikacji.
- Siła hasła jest przedstawiona w formie czerwonych, żółtych i zielonych wskaźników.

Ikona programu **Password Manager** jest wyświetlana w lewym górnym rogu ekranu logowania strony internetowej lub aplikacji. Jeśli dla jakiejś strony internetowej lub aplikacji nie zostały jeszcze zdefiniowane dane logowania, na ikonie wyświetli się znak plus.

▲ Kliknij lub naciśnij ikonę **Password Manager**, aby wyświetlić manu kontekstowe, w którym możesz wybrać następujące opcje:

- Dodaj [przykładowadomena.com] do programu Password Manager
- Uruchom program Password Manager
- Ustawienia ikony
- Pomoc

Dla stron internetowych i programów, dla których nie zdefiniowano jeszcze danych logowania.

W menu kontekstowym są wyświetlane następujące opcje:

- **Add [somedomain.com] to the Password Manager** (Dodaj [Przykładowadomena.com] do programu Password Manager) — Pozwala na dodanie informacji logowania do bieżącego ekranu logowania.
- **Open Password Manager** (Uruchom program Password Manager) — Uruchamia program Password Manager.
- **Icon Settings** (Ustawienia ikony) — Pozwala na zdefiniowanie warunków wyświetlania ikony **Password Manager**.
- **Help** (Pomoc) — Wyświetla dokument pomocy programu HP Client Security.

Dla stron internetowych i programów, dla których już zdefiniowano dane logowania.

W menu kontekstowym są wyświetlane następujące opcje:

- **Fill in logon data** (Wprowadź dane logowania) — Wyświetla stronę **Verify your identity** (Zweryfikuj swoją tożsamość). Po pomyślnym uwierzytelnieniu twoje dane logowania są wprowadzane w polach logowania i przesyłane (jeśli przesyłanie zostało określone podczas tworzenia danych logowania lub przy ich ostatniej edycji).
- **Edit Logon** (Edytuj dane logowania) — Pozwala na edycję danych logowania na tej stronie.
- **Add Logon** (Dodaj dane logowania) — Pozwala na dodanie nowego konta do programu Password Manager.
- **Open Password Manager** (Uruchom program Password Manager) — Uruchamia program Password Manager.
- **Help** (Pomoc) — Wyświetla dokument pomocy programu HP Client Security.

UWAGA: Administrator komputera może skonfigurować program HP Client Security w taki sposób, aby podczas weryfikacji tożsamości konieczne było wprowadzenie więcej niż jednego uwierzytelnienia.

Dodawanie danych logowania

Możesz w łatwy sposób dodawać dane logowania dla strony internetowej lub programu poprzez jednokrotne wprowadzenie danych logowania. Od tej pory program Password Manager będzie automatycznie wprowadzał te dane za ciebie. Dane te mogą być wykorzystywane po wejściu na stronę internetową lub do programu.

Aby dodać dane logowania:

1. Otwórz ekran logowania strony internetowej lub programu.
2. Kliknij lub naciśnij ikonę **Password Manager**, a następnie kliknij lub naciśnij jeden z poniższych przycisków, w zależności od tego, czy logujesz się do strony internetowej, czy programu:
   - W przypadku strony internetowej, kliknij lub naciśnij **Add [domain name] to Password Manager** (Dodaj [nazwa domeny] do programu Password Manager).
   - W przypadku programu, kliknij lub naciśnij **Add this logon screen to Password Manager** (Dodaj ten ekran logowania do programu Password Manager).
3. Wprowadź swoje dane logowania. Pola danych logowania na ekranie oraz odpowiadające im pola w oknie dialogowym są oznaczone grubą, pomarańczową krawędzią.
   a. Aby wybrać wcześniej zdefiniowane dane do wprowadzenia w polu logowania, klikaj lub naciskaj strzałki umiejscowione z prawej strony pola.
   b. Aby sprawdzić hasło dla tego logowania, kliknij lub naciśnij **Show password** (Pokaż hasło).
   c. Jeśli chcesz wprowadzić dane logowania, lecz nie chcesz aby były przesyłane, odznacz pole wyboru **Automatically submit logon data** (Automatycznie przesyłaj dane logowania).
   d. Kliknij lub naciśnij **OK**, aby wybrać metodę uwierzytelnienia, z której chcesz korzystać (linie papilarne, karta inteligentna, karta zbliżeniowa, karta bezstykowa, telefon z funkcją Bluetooth, kod PIN lub hasło) i zaloguj się za pomocą wybranej metody.

      Znak plus jest usuwany z ikony programu **Password Manager**, co oznacza, że dane logowania zostały utworzone.
   e. Jeśli program Password Manager nie wykryje pól logowania, kliknij lub naciśnij **More fields** (Więcej pól).
      - Zaznacz pole obok każdego pola wymaganego przy logowaniu, lub odznacz pola, które nie są potrzebne przy logowaniu.
      - Kliknij lub naciśnij **Close** (Zamknij).

Przy każdym kolejnym wejściu na stronę internetową lub do programu, ikona programu **Password Manager** będzie wyświetlana w lewym górnym rogu ekranu logowania do strony internetowej lub aplikacji, sygnalizując możliwość użycia zarejestrowanych danych logowania w celu zalogowania na stronie lub w programie.

Edytowanie danych logowania

Aby edytować dane logowania:

1. Otwórz ekran logowania strony internetowej lub programu.
2. Aby wyświetlić pole dialogowe, w którym możesz edytować informacje dotyczące logowania, kliknij lub naciśnij ikonę programu **Password Manager**, a następnie kliknij lub naciśnij **Edit Logon** (Edytuj dane logowania).

   Pola danych logowania na ekranie oraz odpowiadające im pola w oknie dialogowym są oznaczone grubą, pomarańczową krawędzią.

   Możesz również edytować informacje o koncie z poziomu strony Password Manager, klikając lub naciskając dane logowania, aby wyświetlić opcje edytowania, a następnie wybierając **Edit** (Edytuj).
3. Edytowanie informacji o logowaniu.
   - Aby edytować pole **Account name** (Nazwa konta), wprowadź nową nazwę konta.
   - Aby dodać lub edytować pole **Category** (Kategoria), wprowadź lub zmodyfikuj nazwę w polu **Category** (Kategoria).
   - Aby wybrać pole logowania **Username** (Nazwa użytkownika) i wypełnić je wcześniej zdefiniowanymi danymi, kliknij lub naciśnij strzałkę w dół umiejscowioną na prawo od pola.

     Wcześniej zdefiniowane dane są dostępne tylko w przypadku edycji danych logowania za pomocą komendy Edytuj w menu kontekstowym ikony programu Password Manager.
   - Aby wybrać pole logowania **Password** (Hasło) i wypełnić je wcześniej zdefiniowanymi danymi, kliknij lub naciśnij strzałkę w dół umiejscowioną na prawo od pola.

     Wcześniej zdefiniowane dane są dostępne tylko w przypadku edycji danych logowania za pomocą komendy Edytuj w menu kontekstowym ikony programu Password Manager.
   - Aby dodać dodatkowe pola z ekranu do danych logowania, kliknij lub naciśnij **More fields** (Więcej pól).
   - Aby sprawdzić hasło dla tego logowania, kliknij lub naciśnij ikonę **Show password** (Pokaż hasło).
   - Jeśli chcesz wprowadzić dane logowania, lecz nie chcesz aby były przesyłane, odznacz pole wyboru **Automatically submit logon data** (Automatycznie przesyłaj dane logowania).
   - Aby oznaczyć dane logowania jako dane z zagrożonym hasłem, zaznacz pole wyboru **This password is compromised** (To hasło jest zagrożone).

     Po zapisaniu zmian wszystkie pozostałe dane logowania korzystające z tego hasła również zostaną oznaczone jako zagrożone. Możesz wejść na każde konto, którego dotyczy problem i w razie potrzeby zmienić hasło.
4. Kliknij lub naciśnij **OK**.

Korzystanie z menu Quick Links programu Password Manager

Password Manager zapewnia możliwość szybkiego i łatwego otwierania stron internetowych i programów, dla których zdefiniowano dane logowania. Dwukrotnie kliknij lub naciśnij dane logowania do programu lub strony internetowej z poziomu menu **Password Manager Quick Links** (Szybkie łącza programu Password Manager) lub z poziomu strony programu Password Manager w obrębie aplikacji HP Client Security, aby otworzyć ekran logowania i wprowadzić dane logowania.

Utworzone dane logowania są automatycznie dodawane do menu **Quick Links** (Szybkie łącza) programu Password Manager.

Aby wyświetlić menu **Quick Links** (Szybkie łącza):

- Naciśnij skrót klawiszowy **Password Manager** – (ustawiony fabrycznie jako Ctrl+klawisz Windows +h). Aby zmienić kombinację klawiszy dostępu, na stronie głównej aplikacji HP Client Security kliknij **Password Manager**, a następnie kliknij lub naciśnij **Settings** (Ustawienia).

Tworzenie kategorii danych logowania

Utwórz jedną lub kilka kategorii, aby uporządkować twoje dane logowania.

Aby przyporządkować dane logowania do danej kategorii:

1. Na stronie głównej aplikacji HP Client Security kliknij lub naciśnij **Windows Password** (Hasło systemu Windows)
2. Kliknij lub naciśnij konto, a następnie kliknij lub naciśnij **Edit** (Edytuj).
3. Wprowadź nazwę kategorii w polu **Category** (Kategoria).
4. Kliknij lub naciśnij **Save** (Zapisz).

Aby usunąć konto z danej kategorii:

1. Na stronie głównej aplikacji HP Client Security kliknij lub naciśnij **Windows Password** (Hasło systemu Windows)
2. Kliknij lub naciśnij konto, a następnie kliknij lub naciśnij **Edit** (Edytuj).
3. Usuń nazwę kategorii z pola **Category** (Kategoria).
4. Kliknij lub naciśnij **Save** (Zapisz).

Aby zmienić nazwę kategorii:

1. Na stronie głównej aplikacji HP Client Security kliknij lub naciśnij **Windows Password** (Hasło systemu Windows)
2. Kliknij lub naciśnij konto, a następnie kliknij lub naciśnij **Edit** (Edytuj).
3. Zmień nazwę kategorii w polu **Category** (Kategoria).
4. Kliknij lub naciśnij **Save** (Zapisz).

Zarządzanie danymi logowania

Program Password Manager umożliwia łatwe zarządzanie danymi logowania (nazwami użytkowników i hasłami), a także kontami zawierającymi wiele danych logowania z poziomu jednej, centralnej lokalizacji.

Twoje dane logowania są wyszczególnione na liście widocznej na stronie programu Password Manager.

Aby zarządzać danymi logowania:

1. Na stronie głównej aplikacji HP Client Security kliknij lub naciśnij **Windows Password** (Hasło systemu Windows).
2. Kliknij lub naciśnij istniejące dane logowania, a następnie wybierz jedną z poniższych opcji i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie:
   - **Edit** (Edytuj) — Edytuj dane logowania. Aby uzyskać więcej informacji, zobacz Edytowanie danych logowania na stronie 23.
   - **Log in** (Zaloguj) — Zaloguj się na wybranym koncie.
   - **Delete** (Usuń) — Usuń dane logowania z wybranego konta.

Aby dodać dodatkowe dane logowania do strony internetowej lub programu:

1. Otwórz ekran logowania strony internetowej lub programu.
2. Kliknij lub naciśnij ikonę programu **Password Manager**, aby wyświetlić menu kontekstowe.
3. Kliknij lub naciśnij **Add Logon** (Dodaj dane logowania), a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Ocena siły hasła

Używanie silnych haseł do logowania się do stron internetowych i programów stanowi ważny aspekt ochrony tożsamości.

Program Password Manager sprawia, że monitorowanie i zwiększanie bezpieczeństwa jest proste dzięki automatycznym analizom siły poszczególnych haseł, wykorzystywanych do logowania do stron internetowych i programów.

Gdy wprowadzasz hasło podczas tworzenia konta i danych logowania do programu Password Manager, poniżej wpisywanego hasła znajduje się kolorowy pasek, który wskazuje siłę hasła. Poszczególne kolory oznaczają następujące wartości:

- **Red** (Czerwony) — Niska
- **Yellow** (Żółty) — Średnia
- **Green** (Zielony) — Wysoka

Ustawienia ikony programu Password Manager

Program Password Manager próbuje identyfikować ekrany logowania poszczególnych stron internetowych i programów. Jeśli wykryje ekran logowania, dla którego nie zostały zdefiniowane dane

logowania, poprosi o dodanie danych logowania dla tego ekranu poprzez wyświetlenie ikony **Password Manager** z znakiem plus.

1. Kliknij lub naciśnij ikonę, a następnie kliknij lub naciśnij **Icon Settings** (Ustawienia ikony), aby zdefiniować, w jaki sposób program Password Manager ma reagować na inne strony z niezdefiniowanymi danymi logowania.

   - **Prompt to add logons for logon screens** (Przypominaj, aby dodawać dane logowania dla ekranów logowania) — Kliknij lub naciśnij tę opcję, a program Password Manager będzie o dodawanie danych logowania dla ekranów logowania, dla których nie zostały jeszcze zdefiniowane.
   - **Exclude this screen** (Wyklucz ten ekran) — Zaznacz to pole, aby program Password Manager nie prosił o dodanie danych logowania do tego ekranu logowania.
   - **Do not prompt to add logons for logon screens** (Nie przypominaj o możliwości dodawania danych logowania dla ekranów logowania) — Wybierz przycisk opcji.

2. Aby dodać dane logowania dla ekranu logowania, który został wcześniej wykluczony:

   a. Zaloguj się na wykluczonej wcześniej stronie.

   b. Aby Password Manager zapamiętał hasło dla danej strony internetowej, kliknij lub naciśnij **Pamiętaj** w wyskakującym oknie dialogowym by zapisać hasło i utworzyć dane logowania dla strony.

3. Aby uzyskać dostęp do dodatkowych ustawień programu Password Manager, kliknij lub naciśnij ikonę Password Manager, kliknij lub naciśnij **Open Password Manager** (Uruchom program Password Manager), a następnie kliknij lub naciśnij **Settings** (Ustawienia) na stronie programu Password Manager.

Importowanie i eksportowanie danych logowania

Strona importowania i eksportowania w programie HP Password Manager służy do importowania danych logowania zapisanych w przeglądarkach internetowych twojego komputera. Można również importować dane z kopii zapasowej programu HP Client Security oraz eksportować je do kopii zapasowej programu HP Client Security.

▲ Aby uruchomić stronę importowania i eksportowania, kliknij lub naciśnij **Import and export** (Importowanie i eksportowanie) na stronie programu Password Manager.

Aby zaimportować hasła z przeglądarki internetowej:

1. Kliknij lub naciśnij przeglądarkę, z której chcesz zaimportować hasła (zostaną wyświetlone wyłącznie obecnie zainstalowane przeglądarki).
2. Odznacz pola wyboru, dla kont, których nie chcesz importować haseł.
3. Kliknij lub naciśnij **Importuj**.

Importowanie/eksportowanie danych logowania z/do kopii zapasowej programu HP Client Security może zostać zrealizowane poprzez powiązane łącza (w obrębie **Other Options**) (Inne opcje) na stronie importowania i eksportowania.

UWAGA: Ta funkcja umożliwia jedynie importowanie i eksportowanie danych z programu Password Manager. Aby uzyskać dodatkowe informacje na temat wykonywania kopii zapasowych i przywracania danych z programu HP Client Security, patrz Tworzenie kopii zapasowych i odzyskiwanie danych na stronie 31.

Aby zaimportować dane z pliku kopii zapasowej programu HP Client Security:

1. Na stronie importowania i eksportowania w programie HP Password Manager kliknij lub naciśnij **Import data from an HP Client Security backup file** (Importuj dane z pliku kopii zapasowej programu HP Client Security).
2. Zweryfikuj swoją tożsamość.
3. Wybierz wcześniej utworzony plik kopii zapasowej lub wprowadź ścieżkę do pliku w dostępnym polu, a następnie kliknij lub naciśnij **Browse** (Przeglądaj).
4. Wprowadź hasło wykorzystywane do ochrony pliku, a następnie kliknij lub naciśnij **Next** (Dalej).
5. Kliknij lub naciśnij **Restore** (Przywróć).

Aby wyeksportować dane do pliku kopii zapasowej HP Client Security:

1. Na stronie importowania i eksportowania w programie HP Password Manager kliknij lub naciśnij **Import data from an HP Client Security backup file** (Eksportuj dane z pliku kopii zapasowej programu HP Client Security).
2. Zweryfikuj swoją tożsamość, a następnie kliknij lub naciśnij **Next** (Dalej).
3. Wprowadź nazwę pliku kopii zapasowej. Domyślnie plik ten jest zapisywany w folderze Dokumenty. Aby wybrać inną lokalizację, kliknij lub naciśnij **Browse** (Przeglądaj).
4. Wprowadź i potwierdź hasło służące do ochrony pliku, a następnie kliknij lub naciśnij **Save** (Zapisz).

Ustawienia

Możesz zdefiniować ustawienia w celu spersonalizowania programu Password Manager:

- **Prompt to add logons for logon screens** (Przypominaj o dodawaniu danych logowania dla ekranów logowania) — Ikona programu **Password Manager** oznaczona znakiem plus jest wyświetlana zawsze, gdy zostanie wykryty ekran logowania strony internetowej lub programu, informując o możliwości dodania danych logowania dla tego ekranu logowania w menu **Logons** (Dane logowania).

  Aby wyłączyć tę funkcję, odznacz pole wyboru znajdujące się obok **Prompt to add logons for logon screens** (Przypominaj o dodawaniu danych logowania dla ekranów logowania).

- **Otwórz program Password Manager skrótem Ctrl+Win+h** – domyślny skrót otwierający manu programu **Password Manager Quick Links** to Ctrl+klawisz Windows+h.

  Aby zmienić kombinację klawiszy skrótu, kliknij lub naciśnij tę opcję, a następnie wprowadź nową kombinację klawiszy. Kombinacja ta może zawierać jeden lub więcej z poniższych klawiszy: Klawisze ctrl,alt, lub shift, oraz wszystkie litery i cyfry.

  Nie można stosować kombinacji klawiszy skrótu zarezerwowanych dla systemu Windows lub aplikacji zainstalowanych w systemie Windows.

- Aby powrócić do ustawień fabrycznych, kliknij lub naciśnij **Restore defaults** (Przywróć ustawienia fabryczne).

Ustawienia zaawansowane

Administratorzy mogą uzyskać dostęp do poniższych opcji, wybierając ikonę **Gear** (Ustawienia) na stronie głównej programu HP Client Security.

- **Administrator Policies** (Zasady administratora) — Umożliwia konfigurację danych logowania i zasad sesji dla administratorów.
- **Standard User Policies** (Zasady zwykłego użytkownika) — Umożliwia konfigurację danych logowania i zasad sesji dla zwykłych użytkowników.
- **Security Features** (Funkcje bezpieczeństwa) — Pozwala na zwiększenie bezpieczeństwa komputera poprzez ochronę konta systemu Windows za pomocą silnego uwierzytelnienia i/lub aktywacji uwierzytelnienia przed rozruchem systemu operacyjnego Windows.
- **Użytkownicy** — Pozwala na zarządzanie użytkownikami i ich danymi uwierzytelniającymi.
- **My Policies** (Moje zasady) — Pozwala na przeglądanie zasad uwierzytelniania oraz statusu rejestracji.
- **Backup and Restore** (Kopia zapasowa i odzyskiwanie) — Pozwala na wykonanie kopii zapasowej i odzyskanie danych programu HP Client Security.
- **Informacje o HP Client Security** — Wyświetla informacje na temat wersji HP Client Security.

Zasady administratora

Możesz konfigurować zasady logowania i zasady sesji dla administratorów na tym komputerze. Ustalone tu zasady logowania decydują o sposobach uwierzytelniania wymaganych od lokalnych administratorów w celu zalogowania się do systemu Windows. Ustalone tu zasady sesji decydują o sposobach uwierzytelniania wymaganych od lokalnych administratorów w celu zweryfikowania tożsamości podczas sesji systemu Windows.

Domyślnie wszystkie nowe i zmienione zasady są wprowadzane natychmiast po kliknięciu lub naciśnięciu **Apply** (Zastosuj).

Aby dodać nową zasadę:

1. Na stronie głównej programu HP Client Security kliknij lub naciśnij ikonę **Gear** (Ustawienia).
2. Na stronie ustawień zaawansowanych kliknij lub naciśnij **Administrator Policies** (Zasady administratora).
3. Kliknij lub naciśnij **Add new policy** (Dodaj nową zasadę).
4. Kliknij strzałką w dół, aby wybrać uwierzytelnienie podstawowe i dodatkowe (opcjonalnie) dla nowej zasady, a następnie kliknij lub naciśnij **Add** (Dodaj).
5. Kliknij **Zastosuj**.

Aby opóźnić wprowadzenie nowej lub zmienionej zasady:

1. Kliknij lub naciśnij **Enforce this policy immediately** (Wprowadź tę zasadę natychmiast).
2. Wybierz **Enforce this policy on the specific date** (Wybierz tę zasadę w określonym dniu).
3. Wprowadź datę wprowadzenia zasady lub zaznacz datę na wyskakującym kalendarzu.
4. W razie potrzeby wybierz, kiedy ma zostać wysłane do użytkowników przypomnienie o nowej zasadzie.
5. Kliknij **Zastosuj**.

Zasady zwykłego użytkownika

Możesz konfigurować zasady logowania i zasady sesji dla zwykłych użytkowników na tym komputerze. Ustalone tu zasady logowania decydują o sposobach uwierzytelniania wymaganych od zwykłych użytkowników w celu zalogowania się do systemu Windows. Ustalone tu zasady sesji decydują o sposobach uwierzytelniania wymaganych od zwykłych użytkowników w celu zweryfikowania tożsamości podczas sesji systemu Windows.

Domyślnie wszystkie nowe i zmienione zasady są wprowadzane natychmiast po kliknięciu lub naciśnięciu **Apply** (Zastosuj).

Aby dodać nową zasadę:

1. Na stronie głównej programu HP Client Security kliknij lub naciśnij ikonę **Gear** (Ustawienia).
2. Na stronie ustawienia zaawansowane kliknij lub naciśnij **Administrator Policies** (Zasady administratora).
3. Kliknij lub naciśnij **Add new policy** (Dodaj nową zasadę).
4. Kliknij strzałką w dół, aby wybrać uwierzytelnienie podstawowe i dodatkowe (opcjonalnie) dla nowej zasady, a następnie kliknij lub naciśnij **Add** (Dodaj).
5. Kliknij **Zastosuj**.

Aby opóźnić wprowadzenie nowej lub zmienionej zasady:

1. Kliknij lub naciśnij **Enforce this policy immediately** (Wprowadź tę zasadę natychmiast).
2. Wybierz **Enforce this policy on the specific date** (Wybierz tę zasadę w określonym dniu).
3. Wprowadź datę wprowadzenia zasady lub zaznacz datę na wyskakującym kalendarzu.
4. W razie potrzeby wybierz, kiedy ma zostać wysłane do użytkowników przypomnienie o nowej zasadzie.
5. Kliknij **Zastosuj**.

Opcje zabezpieczeń

Możesz uaktywnić funkcje programu HP Client Security, które pomogą ci chronić komputer przed nieautoryzowanym dostępem.

Aby skonfigurować funkcje bezpieczeństwa:

1. Na stronie głównej programu HP Client Security kliknij lub naciśnij ikonę **Gear** (Ustawienia).
2. Na stronie ustawień zaawansowanych kliknij lub naciśnij **Security Features** (Opcje zabezpieczeń).

3. Uaktywnij funkcje bezpieczeństwa poprzez zaznaczenie odpowiednich pól wyboru, a następnie kliknij lub naciśnij **Apply** (Zastosuj). Im więcej funkcji bezpieczeństwa wybierzesz, tym bardziej bezpieczny będzie twój komputer.

   Ustawienia te będą dotyczyć wszystkich użytkowników.

   - **Windows Logon Security** (Bezpieczeństwo logowania do systemu Windows) — Chroni twoje konta systemu Windows przed nieuprawnionym dostępem, żądając uwierzytelnień zdefiniowanych w programie HP Client Security.
   - **Pre-Boot Security (Power-on authentication)** (Bezpieczeństwo przedrozruchowe (Uwierzytelnienie po włączeniu komputera)) — Chroni twój komputer jeszcze przed uruchomieniem systemu Windows. Funkcja ta jest niedostępna, jeśli BIOS danego komputera jej nie obsługuje.
   - **Allow One Step logon** (Zezwalaj na jednostopniowe logowanie) — Ustawienie to pozwala na pominięcie logowania z poziomu ekranu Windows, jeśli uwierzytelnianie zostało przeprowadzone wcześniej podczas rozruchu komputera lub z poziomu programu Drive Encryption.

4. Kliknij lub naciśnij **Użytkownicy**, a następnie kliknij lub naciśnij kafelek użytkownika.

Użytkownicy

Możesz monitorować i zarządzać użytkownikami programu HP Client Security na tym komputerze.

Aby dodać kolejnego użytkownika systemu Windows do programu HP Client Security:

1. Na stronie głównej programu HP Client Security kliknij lub naciśnij ikonę **Gear** (Ustawienia).
2. Na stronie ustawień zaawansowanych kliknij lub naciśnij **Users** (Użytkownicy).
3. Kliknij lub naciśnij **Add another Windows user to HP Client Security** (Dodaj kolejnego użytkownika do programu HP Client Security).
4. Wprowadź nazwę użytkownika, którego chcesz dodać, a następnie kliknij lub naciśnij **OK**.
5. Wprowadź hasło użytkownika systemu Windows.

   Na stronie Użytkownik zostanie wyświetlony kafelek dodanego użytkownika.

Aby usunąć użytkownika systemu Windows z programu HP Client Security:

1. Na stronie głównej programu HP Client Security kliknij lub naciśnij ikonę **Gear** (Ustawienia).
2. Na stronie ustawień zaawansowanych kliknij lub naciśnij **Users** (Użytkownicy).
3. Kliknij lub naciśnij nazwę użytkownika, którego chcesz usunąć.
4. Kliknij lub naciśnij **Usuń użytkownika**, a następnie kliknij lub naciśnij **Tak** aby potwierdzić.

Aby wyświetlić zasady logowania i sesji narzucone obowiązujące użytkownika:

▲ Kliknij lub naciśnij **Użytkownicy**, a następnie kliknij lub naciśnij kafelek użytkownika.

Moje zasady

Możesz wyświetlić zasady uwierzytelniania oraz status rejestracji. Na stronie Moje zasady umieszczono łącza do stron Zasady administratorów oraz Zasady zwykłego użytkownika.

1. Na stronie głównej programu HP Client Security kliknij lub naciśnij ikonę **Gear** (Ustawienia).
2. Na stronie ustawień zaawansowanych kliknij lub naciśnij **My Policies** (Moje zasady).

   Zostaną wyświetlone zasady logowania i sesji obowiązujące obecnie zalogowanego użytkownika.

Na stronie Moje zasady umieszczono dodatkowo łącza do Zasady administratora na stronie 28 oraz do Zasady zwykłego użytkownika na stronie 29.

Tworzenie kopii zapasowych i odzyskiwanie danych

Zalecamy regularne tworzenie kopii zapasowych danych programu HP Client Security. Częstotliwość wykonywania kopii zapasowych zależy od tego, jak często dane te są zmieniane. Na przykład jeśli nowe dane logowania są dodawane codziennie, kopię zapasową danych należy również aktualizować codziennie.

Pliki kopii zapasowych mogą być również wykorzystywane podczas migracji z jednego komputera na drugi (eksportowanie i importowanie danych).

UWAGA: Kopie zapasowe są tworzone w taki sposób jedynie dla programu Password Manager. Program Drive Encryption korzysta z innej, niezależnej metody tworzenia kopii zapasowych. Dane programu Device Access Manager i informacje na temat uwierzytelniania za pomocą czytnika linii papilarnych nie są umieszczane w kopii zapasowej.

Program HP Client Security musi być zainstalowany na każdym komputerze, który zaimportuje dane z kopii zapasowej w celu ich odzyskania.

Aby utworzyć kopię zapasową danych:

1. Na stronie głównej programu HP Client Security kliknij lub naciśnij ikonę **Gear** (Ustawienia).
2. Na stronie ustawień zaawansowanych kliknij lub naciśnij **Administrator Policies** (Zasady administratora).
3. Kliknij lub naciśnij **Backup and Restore** (Kopia zapasowa i przywracanie).
4. Kliknij lub naciśnij **Backup** (Kopia zapasowa), a następnie zweryfikuj swoją tożsamość.
5. Wybierz moduł oprogramowania, którego dane chcesz umieścić w pliku kopii zapasowej, a następnie kliknij lub naciśnij **Next** (Dalej).
6. Wprowadź nazwę pliku magazynu. Domyślnie plik ten jest zapisywany w folderze Dokumenty. Aby wybrać inną lokalizację, kliknij lub naciśnij **Browse** (Przeglądaj).
7. Wprowadź i potwierdź hasło do ochrony pliku kopii zapasowej.
8. Kliknij lub naciśnij **Save** (Zapisz).

Aby przywrócić dane:

1. Na stronie głównej programu HP Client Security kliknij lub naciśnij ikonę **Gear** (Ustawienia).
2. Na stronie ustawień zaawansowanych kliknij lub naciśnij **Administrator Policies** (Zasady administratora).
3. Kliknij lub naciśnij **Backup and Restore** (Kopia zapasowa i przywracanie).
4. Wybierz **Restore** (Przywracanie), a następnie zweryfikuj swoją tożsamość.
5. Wybierz wcześniej utworzony plik kopii zapasowej. W widocznym polu wprowadź ścieżkę dostępu. Aby wybrać inną lokalizację, kliknij lub naciśnij **Browse** (Przeglądaj).

6. Wprowadź hasło wykorzystywane do ochrony pliku, a następnie kliknij lub naciśnij **Next** (Dalej).
7. Wybierz moduły oprogramowania, dla których chcesz odzyskać dane.
8. Kliknij lub naciśnij **Restore** (Przywróć).

5 HP Drive Encryption (tylko wybrane modele)

Narzędzie HP Drive Encryption umożliwia szyfrowanie danych przechowywanych na dysku twardym, zapewniając ich całkowitą ochronę. Gdy funkcja Drive Encryption jest aktywna, musisz zalogować się na ekranie logowania Drive Encryption, wyświetlanym przed uruchomieniem systemu Windows®.

Ekran narzędzia HP Client Security pozwala administratorom systemu Windows na włączenie funkcji Drive Encryption, wykonanie kopii zapasowej klucza szyfrującego oraz wybór i rezygnację z szyfrowania określonych dysków lub partycji. Dodatkowe informacje zamieszczono w dokumencie pomocy HP Client Security.

Narzędzie Drive Encryption umożliwia wykonanie następujących zadań:

- Wybór ustawień narzędzia Drive Encryption:
  - Szyfrowanie lub deszyfrowanie pojedynczych dysków lub partycji za pomocą szyfrowania programowego
  - Szyfrowanie lub deszyfrowanie pojedynczych dysków samoszyfrujących za pomocą szyfrowania sprzętowego
  - Dodatkowe zabezpieczenie danych poprzez wyłączenie funkcji Uśpienia lub Wstrzymania. Dzięki temu uwierzytelnienie przedrozruchowe Drive Encryption będzie zawsze wymagane

UWAGA: Narzędzie jest w stanie szyfrować dane tylko na wewnętrznych dyskach SATA i zewnętrznych eSATA.

- Tworzenie kopii zapasowych kluczy szyfrujących
- Odzyskiwanie dostępu do zaszyfrowanego komputera za pomocą zapasowych kluczy szyfrujących i funkcji HP SpareKey
- Aktywacja uwierzytelniania przedrozruchowego Drive Encryption za pomocą hasła, zarejestrowanego odcisku palca lub numeru PIN wybranych kart inteligentnych

Otwieranie narzędzia Drive Encryption

Administratorzy systemu uzyskują dostęp do narzędzia Drive Encryption poprzez otwarcie aplikacji HP Client Security:

1. Na ekranie startowym kliknij lub naciśnij ikonę aplikacji **HP Client Security** (Windows 8).

   — lub —

   Na pulpicie systemu Windows dwukrotnie kliknij lub naciśnij ikonę **HP Client Security** umieszczoną w obszarze powiadomień, z prawej strony paska zadań.

2. Kliknij lub naciśnij ikonę **Drive Encryption**.

Zadania ogólne

Aktywacja narzędzia Drive Encryption dla standardowych dysków twardych

Informacje na standardowych dysków twardych są szyfrowane za pomocą szyfrowania programowego. W celu zaszyfrowania dysku lub określonej partycji na dysku:

1. Uruchom narzędzie **Drive Encryption**. Aby uzyskać więcej informacji, zobacz Otwieranie narzędzia Drive Encryption na stronie 33.
2. Zaznacz pole wyboru dysku lub partycji, którą chcesz zaszyfrować, a następnie kliknij lub naciśnij **Backup Key** (Klucz zapasowy).

UWAGA: Dla zapewnienia lepszej ochrony zaznacz pole wyboru **Disable sleep mode for increased security** (Dezaktywuj tryb uśpienia dla lepszej ochrony). Po wyłączeniu trybu uśpienia zyskujemy pewność, że żadne dane uwierzytelniające nie są przechowywane w pamięci komputera.

3. Wybierz jedną lub kilka opcji kopii zapasowej, a następnie kliknij lub naciśnij **Backup** (Kopia zapasowa). Aby uzyskać więcej informacji, zobacz Tworzenie kopii zapasowej kluczy szyfrowania na stronie 38.
4. Podczas tworzenia kopii zapasowej klucza szyfrowania możesz kontynuować pracę na komputerze. Nie uruchamiaj ponownie komputera.

UWAGA: Po chwili zostaniesz poproszony o ponowne uruchomienie komputera. Po ponownym uruchomieniu zostanie wyświetlony przedrozruchowy ekran szyfrowania dysku z żądaniem uwierzytelnienia przed uruchomieniem systemu Windows.

Narzędzie Drive Encryption zostaje aktywowane. Szyfrowanie wybranych partycji dyskowych może zająć nawet kilka godzin, w zależności od ich liczby i wielkości.

Dodatkowe informacje zamieszczono w dokumencie pomocy HP Client Security.

Aktywacja narzędzia Drive Encryption dla dysków samoszyfrujących

Dyski samoszyfrujące zgodne z wymogami OPAL Trusted Computing Group, określającymi zasady zarządzania dyskami samoszyfrującymi mogą być szyfrowane zarówno za pomocą szyfrowania programowego, jak i sprzętowego. Proces szyfrowania sprzętowego jest o wiele szybszy niż proces szyfrowania programowego. Jednak w przypadku szyfrowania sprzętowego nie ma możliwości wyboru partycji, które mają zostać zaszyfrowane. Szyfrowany jest cały dysk ze wszystkimi znajdującymi się na nim partycjami.

Tak więc, gdy istnieje konieczność zaszyfrowania jedynie wybranej partycji, należy zastosować szyfrowanie programowe. Należy pamiętać, by odznaczyć pole wyboru **Only allow hardware encryption for Self-Encrypting Drives (SEDs)** (W przypadku dysków samoszyfrujących (SEDs) pozwalaj jedynie na szyfrowanie sprzętowe).

By aktywować narzędzie Drive Encryption dla dysków samoszyfrujących:

1. Uruchom narzędzie **Drive Encryption**. Aby uzyskać więcej informacji, zobacz Otwieranie narzędzia Drive Encryption na stronie 33.
2. Zaznacz pole wyboru dysku, który chcesz zaszyfrować, a następnie kliknij lub naciśnij **Backup Key** (Klucz zapasowy).

UWAGA: Dla zapewnienia lepszej ochrony zaznacz pole wyboru **Disable Sleep Mode for added security** (Dezaktywuj tryb uśpienia dla lepszej ochrony). Po wyłączeniu trybu uśpienia zyskujemy pewność, że żadne dane uwierzytelniające nie są przechowywane w pamięci komputera.

3. Wybierz jedną lub kilka opcji kopii zapasowej, a następnie kliknij lub naciśnij **Backup** (Kopia zapasowa). Aby uzyskać więcej informacji, zobacz Tworzenie kopii zapasowej kluczy szyfrowania na stronie 38.
4. Podczas tworzenia kopii zapasowej klucza szyfrowania możesz kontynuować pracę na komputerze. Nie uruchamiaj ponownie komputera.

UWAGA: W przypadku dysków samoszyfrujących zostanie wyświetlony komunikat o konieczności wyłączenia komputera.

Dodatkowe informacje zamieszczono w dokumencie pomocy HP Client Security.

Dezaktywacja narzędzia Drive Encryption

1. Uruchom narzędzie **Drive Encryption**. Aby uzyskać więcej informacji, zobacz Otwieranie narzędzia Drive Encryption na stronie 33.
2. Odznacz pola wyboru wszystkich zaszyfrowanych dysków, a następnie kliknij lub naciśnij **Apply** (Zastosuj).

   Rozpocznie się dezaktywacja narzędzia Drive Encryption.

UWAGA: Jeśli do zaszyfrowania dysków zostało użyte oprogramowanie szyfrujące, rozpocznie się proces deszyfrowania. Może to zająć nawet kilka godzin, w zależności od liczby i wielkości wybranych partycji dyskowych. Po zakończeniu procesu deszyfrowania, program Drive Encryption zostaje dezaktywowany.

W przypadkach, gdy było stosowane szyfrowanie sprzętowe, proces deszyfrowania jest natychmiastowy, a narzędzie Drive Encryption zostaje dezaktywowane już po kilku minutach.

Po dezaktywacji narzędzia Drive Encryption zostaniesz poproszony o wyłączenie komputera (w przypadku szyfrowania sprzętowego), lub ponowne uruchomienie komputera (w przypadku szyfrowania programowego).

Logowanie po aktywacji narzędzia Drive Encryption

W przypadku włączenia komputera po aktywacji narzędzia Drive Encryption, gdy konto użytkownika jest zarejestrowane, należy zalogować się korzystając z ekranu logowania narzędzia Drive Encryption:

UWAGA: Przy wychodzeniu z trybu uśpienia lub trybu wstrzymania, ekran uwierzytelniania przedrozruchowego Drive Encryption nie jest wyświetlany ani w przypadku szyfrowania programowego, ani sprzętowego. W przypadku szyfrowania sprzętowego istnieje możliwość dezaktywacji trybu uśpienia poprzez wybór opcji **Disable sleep mode for increased security** (Wyłącz tryb uśpienia w celu zwiększenia bezpieczeństwa), co uniemożliwi przechodzenie komputera w stan uśpienia lub wstrzymania, gdy tryby te są włączone w opcjach systemowych.

Przy wychodzeniu z trybu hibernacji, ekran uwierzytelniania przedrozruchowego Drive Encryption jest wyświetlany zarówno w przypadku szyfrowania programowego, jak i sprzętowego.

UWAGA: Jeśli administrator systemu Windows uaktywni opcję BIOS Pre-boot Security dostępną w aplikacji HP Client Security, a jednocześnie opcja jednoetapowego logowania One-Step Logon jest aktywna (domyślnie), do komputera można zalogować się natychmiast po uwierzytelnieniu przedrozruchowym BIOS Pre-boot, bez konieczności ponownego uwierzytelnienia na ekranie logowania narzędzia Drive Encryption.

Logowanie pojedynczego użytkownika:

- ▲ Na stronie **Logon** (Logowanie) wpisz swoje hasło dostępu do systemu Windows, numer PIN karty inteligentnej, klucz zapasowy SpareKey lub przyłóż palec (ten, który został wcześniej zarejestrowany w systemie) do czytnika linii papilarnych.

Logowanie wielu użytkowników:

1. Na stronie **Select user to logon** (Wybierz użytkownika do zalogowania) wybierz z listy rozwijalnej użytkownika, który ma zostać zalogowany, po czym kliknij lub naciśnij **Next** (Dalej).
2. Na stronie **Logon** (Logowanie) wpisz swoje hasło dostępu do systemu Windows, numer PIN karty inteligentnej, lub przyłóż palec (ten, który został wcześniej zarejestrowany w systemie) do czytnika linii papilarnych.

UWAGA: Obsługiwane są następujące karty inteligentne:

Obsługiwane karty inteligentne

- Gemalto Cyberflex Access 64k V2c

UWAGA: W przypadku użycia klucza odzyskiwania do logowania na ekranie logowania narzędzia Drive Encryption, do zalogowania na konto użytkownika systemu Windows będą konieczne dodatkowe dane uwierzytelniające.

Szyfrowanie dodatkowych dysków twardych

Zdecydowanie zalecamy korzystanie z narzędzia HP Drive Encryption w celu ochrony danych zapisanych na dysku twardym. Po aktywacji narzędzia, aby zaszyfrować jakikolwiek dodany dysk twardy lub utworzoną partycję, wykonaj następujące czynności:

1. Uruchom narzędzie **Drive Encryption**. Aby uzyskać więcej informacji, zobacz Otwieranie narzędzia Drive Encryption na stronie 33.
2. W przypadku dysków szyfrowanych programowo wybierz partycje dyskowe do zaszyfrowania.

UWAGA: Procedura ta dotyczy również sytuacji, w których istnieje jeden lub więcej standardowych dysków twardych oraz jeden lub więcej dysków samoszyfrujących.

— lub —

- ▲ W przypadku dysków szyfrowanych programowo wybierz dodatkowe dyski do zaszyfrowania.

Zadania zaawansowane

Zarządzanie narzędziem Drive Encryption (zadanie administratora)

Administratorzy systemu mogą za pomocą narzędzia Drive Encryption przeglądać lub zmieniać status szyfrowania (Zaszyfrowany lub Niezaszyfrowany) wszystkich dysków twardych zainstalowanych w komputerze.

- Gdy narzędzie Drive Encryption posiada status Aktywny, oznacza to, że zostało ono aktywowane i skonfigurowane. Dysk może posiadać jeden z poniższych statusów:

Szyfrowanie programowe

- Niezaszyfrowany
- Zaszyfrowany
- Szyfrowanie
- Deszyfrowanie

Szyfrowanie sprzętowe

- Zaszyfrowany
- Niezaszyfrowany (dla dodatkowych dysków)

Szyfrowanie lub deszyfrowanie pojedynczych partycji dyskowych (tylko szyfrowanie programowe)

Administratorzy systemu Windows mogą wykorzystać narzędzie Drive Encryption do zaszyfrowania jednej lub kilku partycji dysku twardego komputera lub zdeszyfrowania partycji wcześniej zaszyfrowanych.

1. Uruchom narzędzie **Drive Encryption**. Aby uzyskać więcej informacji, zobacz Otwieranie narzędzia Drive Encryption na stronie 33.
2. Na karcie **Drive Status** (Status dysku), zaznacz lub odznacz pole wyboru partycji dyskowej, którą chcesz zaszyfrować lub odszyfrować, a następnie kliknij lub naciśnij **Apply** (Zastosuj).

UWAGA: W trakcie szyfrowania lub deszyfrowania partycji, pasek postępu wyświetla procentowe zaawansowanie procesu.

UWAGA: Partycje dynamiczne nie są obsługiwane. Jeśli któraś z partycji jest wyświetlana jako dostępna, lecz po wybraniu nie może zostać zaszyfrowana, oznacza to, że jest to partycja dynamiczna. Tworzenie partycji dynamicznej polega na spakowaniu partycji podstawowej i utworzeniu nowej partycji z poziomu Zarządzania dyskiem.

Przed rozpoczęciem konwersji partycji podstawowej na dynamiczną, na ekranie zostanie wyświetlone ostrzeżenie.

Zarządzanie dyskiem

- **Nickname** (Nazwa) — Możesz przypisać swoim dyskom lub partycjom nazwy w celu ich łatwiejszej identyfikacji.
- **Disconnected drives** (Dyski odłączone) — Narzędzie Drive Encryption może zidentyfikować dyski, które zostały odłączone od komputera. Każdy dysk po odłączeniu od komputera automatycznie pojawia się na liście Dyski odłączone. Jeśli dysk zostanie powtórnie podłączony do komputera, pojawi się na liście Dyski podłączone.

- Jeśli nie potrzebujesz już śledzić statusu przyłączenia danego dysku po jego odłączeniu, możesz go usunąć z listy Dyski odłączone.
- Narzędzie Drive Encryption zostaje dezaktywowane, gdy pola wyboru wszystkich podłączonych dysków zostaną odznaczone, a lista Dyski odłączone zostanie wyczyszczona.

Kopia zapasowa i odzyskiwanie (zadanie administratora)

Gdy narzędzie Drive Encryption jest aktywne, administratorzy, poprzez stronę Kopia zapasowa klucza szyfrowania systemu, mogą utworzyć kopie zapasowe kluczy szyfrowania na przenośnych nośnikach pamięci oraz przeprowadzić odzyskiwanie kluczy.

Tworzenie kopii zapasowej kluczy szyfrowania

Administratorzy systemu mogą wykonać kopię zapasową klucza szyfrowania dla zaszyfrowanego dysku na przenośnym nośniku pamięci.

⚠ **OSTROŻNIE:** Nośnik pamięci zawierający kopię klucza należy przechowywać w bezpiecznym miejscu, ponieważ w przypadku utraty hasła dostępu i karty inteligentnej przy jednoczesnym braku zarejestrowanego odcisku palca, urządzenie to jako jedyne umożliwi dostęp do zasobów komputera. Dodatkowo, miejsce przechowywania nośnika powinno być zabezpieczone, gdyż umożliwia ono dostęp od systemu Windows komputera.

1. Uruchom narzędzie **Drive Encryption**. Aby uzyskać więcej informacji, zobacz Otwieranie narzędzia Drive Encryption na stronie 33.
2. Zaznacz pole wyboru dysku, a następnie kliknij lub naciśnij **Backup Key** (Klucz zapasowy).
3. Na karcie **Create HP Drive Encryption recovery key** (Utwórz klucz zapasowy HP Drive Encryption) wybierz jedną lub kilka z poniższych opcji:
   - **Removable Storage** (Przenośny nośnik pamięci) — Zaznacz pole wyboru i wybierz przenośny nośnik pamięci, na którym ma zostać zapisana kopia klucza szyfrowania.
   - **SkyDrive** — Zaznacz pole wyboru. By skorzystać z tej opcji, komputer musi być podłączony do Internetu. Zaloguj się na stronie Microsoft SkyDrive, a następnie kliknij lub naciśnij **Yes** (Tak).

     UWAGA: By użyć klucza zapasowego HP Drive Encryption przechowywanego na SkyDrive, musisz go pobrać ze strony SkyDrive na przenośny nośnik pamięci, a następnie włożyć urządzenie do komputera.
   - **TPM** (tylko wybrane modele) — Pozwala na odzyskanie danych za pomocą hasła TPM.

     ⚠ **OSTROŻNIE:** Jeśli hasło TPM zostanie usunięte lub komputer zostanie uszkodzony, utracisz dostęp do kopii zapasowej. Jeśli została wybrana ta metoda, należy wybrać dodatkowo inną metodę tworzenia kopii zapasowej.
4. Kliknij lub naciśnij **Backup** (Kopia zapasowa).

   Klucz szyfrowania zostanie zapisany na wybranym przenośnym nośniku pamięci.

Odzyskiwanie dostępu do komputera za pomocą kluczy zapasowych

Administratorzy mogą odzyskać dostęp do komputera za pomocą klucza zapasowego Drive Encryption, przechowywanego na przenośnym nośniku pamięci, poprzez aktywację lub wybór opcji **Backup Key** (Klucz zapasowy) w narzędziu Drive Encryption.

1. Podłącz przenośny nośnik pamięci, na którym znajduje się klucz zapasowy.
2. Włącz komputer.

3. Gdy pojawi się okno logowania HP Drive Encryption, kliknij lub naciśnij **Recovery** (Odzyskiwanie).
4. Wybierz ścieżkę lub nazwę pliku zawierającego klucz, a następnie kliknij lub naciśnij **Recovery** (Odzyskiwanie).
5. Gdy pojawi się okno dialogowe potwierdzenia, kliknij lub naciśnij **OK**.

   Pojawi się ekran logowania do systemu Windows.

UWAGA: W przypadku użycia klucza odzyskiwania do logowania na ekranie logowania narzędzia Drive Encryption, do zalogowania na konta użytkownika systemu Windows będą konieczne dodatkowe dane uwierzytelniające. Zdecydowanie zaleca się zmianę dotychczasowego hasła po przeprowadzeniu procedury odzyskiwania.

Przeprowadzanie odzyskiwania HP SpareKey Recovery

Przedrozruchowe odzyskiwanie SpareKey Recovery w narzędziu Drive Encryption wymaga odpowiedzi na pytania bezpieczeństwa. Udzielenie prawidłowych odpowiedzi umożliwia dostęp do komputera. Dodatkowe informacje dotyczące ustawień SpareKey Recovery można znaleźć w dokumencie pomocy oprogramowania HP Client Security.

Odzyskiwanie za pomocą opcji HP SpareKey Recovery w przypadku utraty hasła:

1. Włącz komputer.
2. Gdy wyświetlana jest strona programu HP Drive Encryption, przejdź do strony logowania użytkownika.
3. Kliknij przycisk **SpareKey**.

   UWAGA: Jeśli opcja SpareKey nie została aktywowana w aplikacji HP Client Security, przycisk**SpareKey** nie będzie dostępny.
4. Wpisz poprawne odpowiedzi na wyświetlane pytania, a następnie kliknij **Logowanie**.

   Pojawi się ekran logowania do systemu Windows.

UWAGA: W przypadku użycia opcji SpareKey do logowania na ekranie logowania narzędzia Drive Encryption, do zalogowania na konta użytkownika systemu Windows będą konieczne dodatkowe dane uwierzytelniające. Zdecydowanie zaleca się zmianę dotychczasowego hasła po przeprowadzeniu procedury odzyskiwania.

6 HP File Sanitizer (tylko wybrane modele)

File Sanitizer umożliwia bezpieczne niszczenie zasobów (na przykład: danych osobowych lub plików, danych związanych z przeglądaniem stron internetowych lub innych zasobów) znajdujących się na twardym dysku komputera i okresowe oczyszczanie twardego dysku.

Narzędzie File Sanitizer nie może być używane do czyszczenia lub usuwania danych z następujących napędów:

- Dyski półprzewodnikowe (SSD), również w przypadku, gdy woluminy RAID obejmują dysk SSD
- Napędy zewnętrzne podłączone poprzez łącze USB, Firewire lub eSATA

Przy próbie wyczyszczenia dysku lub usunięcia danych z dysku SSD zostanie wyświetlony komunikat ostrzegawczy i żądana operacja nie zostanie wykonana.

Niszczenie

Niszczenie różni się od standardowego usuwania plików w systemie Windows®. Podczas niszczenia zasobu za pomocą narzędzia File Sanitizer, jest on nadpisywany losowymi danymi, co czyni jego odzyskanie praktycznie niemożliwym. Proste usuwanie w systemie Windows może pozostawić cały plik (lub zasób) nietknięty na dysku twardym, lub w stanie umożliwiającym jego odczytanie za pomocą zaawansowanych metod odzyskiwania danych.

Istnieje możliwość konfiguracji automatycznego harmonogramu niszczenia, lub uruchomienia procesu niszczenia ręcznie poprzez wybranie ikony **File Sanitizer** znajdującej się na ekranie głównym aplikacji HP Client Security, bądź też użycie ikony **File Sanitizer** umieszczonej na pulpicie systemu Windows. Aby uzyskać dodatkowe informacje, patrz: Ustawienie harmonogramu niszczenia na stronie 42, Niszczenie za pomocą prawego przycisku na stronie 44, lub Ręczne uruchamianie operacji niszczenia na stronie 45.

UWAGA: Plik .dll jest niszczony i usuwany z systemu tylko wtedy, gdy zostanie przeniesiony do kosza.

Czyszczenie przestrzeni dyskowej

Usuwanie zasobu w systemie Windows nie usuwa całkowicie jego zawartości z dysku twardego. System Windows usuwa jedynie odwołanie do tego zasobu lub informację o jego lokalizacji na dysku twardym. Zawartość zasobu pozostanie na dysku twardym do czasu, gdy inny zasób nadpisze ten sam obszar nowymi informacjami.

Czyszczenie przestrzeni dyskowej pozwala na bezpieczne zapisanie losowych danych na usuniętych zasobach, uniemożliwiając użytkownikom przeglądanie oryginalnej treści usuniętych zasobów.

UWAGA: Czyszczenie przestrzeni dyskowej nie zapewnia dodatkowego bezpieczeństwa dla zniszczonych zasobów.

Istnieje możliwość konfiguracji automatycznego harmonogramu niszczenia, lub zainicjowania procesu czyszczenia przestrzeni dyskowej ręcznie poprzez wybranie ikony **File Sanitizer** znajdującej się na ekranie głównym aplikacji HP Client Security, bądź też użycie ikony **File Sanitizer** umieszczonej na pulpicie systemu Windows. Aby uzyskać dodatkowe informacje, patrz: Ustawienie harmonogramu

czyszczenia przestrzeni dyskowej na stronie 43, Ręczne uruchamianie czyszczenia przestrzeni dyskowej na stronie 45, lub Użycie ikony programu File Sanitizer na stronie 44.

Otwieranie narzędzia File Sanitizer

1. Na ekranie startowym kliknij lub naciśnij ikonę aplikacji **HP Client Security** (Windows 8).

   — lub —

   Na pulpicie systemu Windows dwukrotnie kliknij lub naciśnij ikonę **HP Client Security** umieszczoną w obszarze powiadomień, z prawej strony paska zadań.

2. Na karcie **Data** (Dane) kliknij lub naciśnij **File Sanitizer**.

— lub —

▲ Dwukrotnie kliknij lub naciśnij ikonę **File Sanitizer** na pulpicie systemu Windows.

— lub —

▲ Kliknij prawym przyciskiem i przytrzymaj lub naciśnij i przytrzymaj ikonę **File Sanitizer** umieszczoną na pulpicie systemu Windows, po czym wybierz **Open File Sanitizer** (Uruchom narzędzie File Sanitizer).

Procedury konfiguracji

Shredding (Niszczenie) — Narzędzie File Sanitizer trwale i w sposób bezpieczny usuwa lub niszczy wybrane kategorie zasobów.

1. Na karcie **Shredding** (Niszczenie) zaznacz pola wyboru poszczególnych typów plików, które mają zostać zniszczone lub odznacz pola wyboru dla typów plików, których nie planujesz usuwać.

   - **Recycle Bin** (Kosz) — Niszczy wszystkie elementy znajdujące się w koszu.
   - **Temporary system files** (Tymczasowe pliki systemowe) — Niszczy wszystkie pliki znajdujące się w katalogu tymczasowych plików systemowych. Przedstawione zmienne środowiskowe są wyszukiwane zgodnie z podaną poniżej kolejnością, a pierwsza odnaleziona ścieżka jest uznawana za katalog systemowy:
     - TMP
     - TEMP
   - **Temporary Internet files** (Tymczasowe pliki internetowe) — Niszczy kopie stron internetowych, zdjęć, oraz pliki multimedialne przechowywane przez przeglądarki internetowe w celu przyspieszenia ich działania.
   - **Cookies** (Ciasteczka) — Niszczy wszystkie pliki zapisywane na dysku na żądanie stron internetowych w celu zapamiętania preferencji i ustawień, jak na przykład danych logowania.

2. W celu rozpoczęcia niszczenia zasobów kliknij lub naciśnij **Shred** (Zniszcz).

Bleaching (Czyszczenie) — Nadpisuje losowe dane w celu zwiększenia dostępnej przestrzeni i uniemożliwia odzyskanie usuniętych zasobów.

▲ Aby rozpocząć czyszczenie, kliknij lub naciśnij **Bleach** (Wyczyść).

File Sanitizer Options (Opcje programu File Sanitizer) — Zaznacz odpowiednie pola wyboru, by aktywować poniższe opcje lub odznacz, by je dezaktywować:

- **Enable Desktop icon** (Pokaż ikonę na pulpicie) — Wyświetla ikonę programu na pulpicie systemu Windows.
- **Enable right-click** (Aktywuj opcję „prawy przycisk”) — Pozwala na wybór karty **HP File Sanitizer – Shred** (HP File Sanitizer – Niszczenie) poprzez kliknięcie (lub naciśnięcie) i przytrzymanie danego zasobu.
- **Ask for Windows password before manual shredding** (Pytaj o hasło systemu Windows przed rozpoczęciem niszczenia ręcznego) — Aktywuje uwierzytelnianie za pomocą hasła systemu Windows przed ręcznym zniszczeniem zasobu.
- **Shred Cookies and Temporary Internet Files on browser close** (Zniszcz ciasteczka i tymczasowe pliki internetowe przy zamykaniu przeglądarki) — Podczas zamykania przeglądarki internetowej niszczy wszystkie wybrane zasoby związane z aktywnością internetową, jak na przykład historię przeglądanych stron.

Ustawienie harmonogramu niszczenia

Istnieje możliwość zdefiniowania czasu, w którym automatyczne niszczenie zasobów ma zostać aktywowane. Można również zniszczyć wybrane zasoby ręcznie w dowolnie wybranym momencie. Więcej informacji można znaleźć w części Procedury konfiguracji na stronie 41.

1. Otwórz File Sanitizer, a następnie kliknij lub naciśnij **Settings** (Ustawienia).
2. By ustawić czas niszczenia wybranych zasobów według**Shred Schedule** (Harmonogramu niszczenia), wybierz**Never** (Nigdy), **Once** (Jednorazowo), **Daily** (Codziennie), **Weekly** (Raz w tygodniu) lub **Monthly** (Raz w miesiącu), a następnie wybierz dzień i godzinę:
   a. Kliknij lub naciśnij pole godziny, minut lub AM/PM (przed południem/po południu).
   b. Przesuwaj aż do momentu wyświetlenia żądanej wartości na tym samym poziomie co inne pola.
   c. Kliknij lub naciśnij białą przestrzeń otaczającą pola ustawień godziny.
   d. Powtórz tę czynność dla innych pól, aż do ustawienia żądanych wartości harmonogramu.
3. Na liście obiektów przeznaczonych do automatycznego niszczenia znajdują się cztery typy zasobów:
   - **Recycle Bin** (Kosz) — Niszczy wszystkie elementy znajdujące się w koszu.
   - **Temporary system files** (Tymczasowe pliki systemowe) — Niszczy wszystkie pliki znajdujące się w katalogu tymczasowych plików systemowych. Przedstawione zmienne środowiskowe są wyszukiwane zgodnie z podaną poniżej kolejnością, a pierwsza odnaleziona ścieżka jest uznawana za katalog systemowy:
     - TMP
     - TEMP
   - **Temporary Internet files** (Tymczasowe pliki internetowe) — Niszczy kopie stron internetowych, zdjęć, oraz pliki multimedialne przechowywane przez przeglądarki internetowe w celu przyspieszenia ich działania.
   - **Cookies** (Ciasteczka) — Niszczy wszystkie pliki zapisywane na dysku na żądanie stron internetowych w celu zapamiętania preferencji i ustawień, jak na przykład danych logowania.

Zaznaczone zasoby zostaną automatycznie zniszczone w czasie określonym w harmonogramie niszczenia.

4. Wybieranie innych zasobów do zniszczenia:

   a. Na karcie **Scheduled Shred List** (Lista zasobów do automatycznego zniszczenia) kliknij lub naciśnij**Add folder** (Dodaj katalog), a następnie przejdź do wybranego pliku lub katalogu.

   b. Kliknij lub naciśnij **Open** (Otwórz), a następnie kliknij lub naciśnij **OK**.

   By usunąć określony zasób z listy zasobów do automatycznego zniszczenia, należy odznaczyć przypisane do niego pole wyboru.

Ustawienie harmonogramu czyszczenia przestrzeni dyskowej

Czyszczenie przestrzeni dyskowej nie zapewnia dodatkowego bezpieczeństwa dla zniszczonych zasobów.

1. Otwórz File Sanitizer, a następnie kliknij lub naciśnij **Settings** (Ustawienia).
2. Aby zaplanować przyszłe oczyszczanie dysku twardego, w zakładce **Bleach Schedule** (Harmonogram oczyszczania), wybierz **Nigdy**, **Jednorazowo**, **Codziennie**, **Co tydzień** lub **Co miesiąc**, a następnie wybierz dzień i czas.

   a. Kliknij lub naciśnij pole godziny, minut lub AM/PM (przed południem/po południu).

   b. Przesuwaj aż do momentu wyświetlenia żądanego czasu na tym samym poziomie co inne pola.

   c. Kliknij lub naciśnij białą przestrzeń otaczającą pola ustawień godziny.

   d. Powtarzaj tę czynność, aż do ustawienia żądanych wartości harmonogramu.

UWAGA: Proces czyszczenia przestrzeni dyskowej może trwać dosyć długo. Należy się upewnić, że komputer w tym czasie jest podłączony do zasilania sieciowego. Mimo że proces czyszczenia przestrzeni dyskowej odbywa się w tle, zwiększone użycie procesora może mieć wpływ na działanie komputera. Czyszczenie przestrzeni dyskowej może odbywać się w czasie, gdy komputer nie jest używany.

Ochrona plików przed zniszczeniem

W celu ochrony plików i katalogów przed zniszczeniem:

1. Otwórz File Sanitizer, a następnie kliknij lub naciśnij **Settings** (Ustawienia).
2. Na karcie **Never Shred List** (Lista zasobów chronionych przed zniszczeniem) kliknij lub naciśnij **Add folder** (Dodaj katalog), a następnie przejdź do wybranego pliku lub katalogu.
3. Kliknij lub naciśnij **Open** (Otwórz), a następnie kliknij lub naciśnij **OK**.

UWAGA: Pliki tę będą chronione, dopóki nie zostaną usunięte z listy.

By usunąć daną pozycję z listy zasobów chronionych przed zniszczeniem, odznacz stosowne pole wyboru.

Zadania ogólne

File Sanitizer można wykorzystywać do wykonywania następujących czynności:

- **Użycie ikony File Sanitizer do rozpoczęcia procesu niszczenia plików** — Przeciągnij wybrany plik na ikonę **File Sanitizer** umieszczoną na pulpicie systemu Windows. Aby uzyskać dodatkowe informacje, patrz: Użycie ikony programu File Sanitizer na stronie 44.
- **Ręczne niszczenie określonych zasobów lub wszystkich wybranych zasobów** — Niszczenie wybranych pozycji w dowolnym czasie bez konieczności oczekiwania na niszczenie automatyczne. Aby poznać szczegóły, patrz Niszczenie za pomocą prawego przycisku na stronie 44 lub Ręczne uruchamianie operacji niszczenia na stronie 45.
- **Ręczne uruchomienie czyszczenia przestrzeni dyskowej** — Ręczne uruchomienie czyszczenia przestrzeni dyskowej w dowolnym momencie. Aby uzyskać dodatkowe informacje, patrz: Ręczne uruchamianie czyszczenia przestrzeni dyskowej na stronie 45.
- **Przegląd plików dziennika** — Przeglądanie plików dziennika generowanych podczas operacji niszczenia zasobów i czyszczenia przestrzeni dyskowej. Aby uzyskać dodatkowe informacje, patrz: Przeglądanie plików dziennika na stronie 45.

UWAGA: Proces niszczenia zasobów lub czyszczenia przestrzeni dyskowej może trwać dosyć długo. Mimo że proces niszczenia zasobów i czyszczenia przestrzeni dyskowej odbywa się w tle, zwiększone użycie procesora może mieć wpływ na działanie komputera.

Użycie ikony programu File Sanitizer

OSTROŻNIE: Nie ma możliwości odzyskania zniszczonych zasobów. Przy wyborze zasobów do ręcznego zniszczenia należy postępować z daleko idącą ostrożnością.

Po ręcznym uruchomieniu operacji niszczenia zasobów zostają zniszczone wszystkie elementy ze standardowej listy elementów umieszczonej w widoku File Sanitizer (patrz Procedury konfiguracji na stronie 41).

Operację niszczenia ręcznego można wykonać w jeden z poniższych sposobów:

1. Otwórz File Sanitizer (patrz Otwieranie narzędzia File Sanitizer na stronie 41), a następnie kliknij lub naciśnij **Shred** (Zniszcz).
2. Po wyświetleniu komunikatu potwierdzającego upewnij się, że zasoby, które chcesz zniszczyć są zaznaczone, a następnie kliknij lub naciśnij **OK**.

— lub —

1. Kliknij prawym przyciskiem i przytrzymaj lub naciśnij i przytrzymaj ikonę **File Sanitizer** na pulpicie systemu Windows, a następnie kliknij lub przyciśnij **Shred Now** (Zniszcz teraz).
2. Po wyświetleniu okna dialogowego z potwierdzeniem upewnij się, że zasoby które chcesz zniszczyć są zaznaczone, a następnie kliknij lub naciśnij**Shred** (Zniszcz).

Niszczenie za pomocą prawego przycisku

OSTROŻNIE: Nie ma możliwości odzyskania zniszczonych zasobów. Przy wyborze zasobów do ręcznego zniszczenia należy postępować z daleko idącą ostrożnością.

Jeśli w widoku programu File Sanitizer wybrano opcję **Enable right-click shredding** (Aktywuj niszczenie za pomocą prawego przycisku) można niszczyć zasoby w następujący sposób:

1. Przejdź do dokumentu lub katalogu, który ma zostać zniszczony.
2. Kliknij prawym przyciskiem i przytrzymaj lub naciśnij i przytrzymaj plik lub katalog, a następnie wybierz **HP File Sanitizer – Shred** (HP File Sanitizer – Niszczenie).

Ręczne uruchamianie operacji niszczenia

⚠ **OSTROŻNIE:** Nie ma możliwości odzyskania zniszczonych zasobów. Przy wyborze zasobów do ręcznego zniszczenia należy postępować z daleko idącą ostrożnością.

Po ręcznym uruchomieniu operacji niszczenia zasobów zostają zniszczone wszystkie elementy ze standardowej listy elementów umieszczonej w widoku File Sanitizer (patrz Procedury konfiguracji na stronie 41).

Operację niszczenia ręcznego można wykonać w jeden z poniższych sposobów:

1. Otwórz File Sanitizer (patrz Otwieranie narzędzia File Sanitizer na stronie 41), a następnie kliknij lub naciśnij **Shred** (Zniszcz).
2. Po wyświetleniu komunikatu potwierdzającego upewnij się, że zasoby, które chcesz zniszczyć są zaznaczone, a następnie kliknij lub naciśnij **OK**.

— lub —

1. Kliknij prawym przyciskiem i przytrzymaj lub naciśnij i przytrzymaj ikonę **File Sanitizer** na pulpicie systemu Windows, a następnie kliknij lub przyciśnij **Shred Now** (Zniszcz teraz).
2. Po wyświetleniu okna dialogowego z potwierdzeniem upewnij się, że zasoby które chcesz zniszczyć są zaznaczone, a następnie kliknij lub naciśnij **Shred** (Zniszcz).

Ręczne uruchamianie czyszczenia przestrzeni dyskowej

Po ręcznym uruchomieniu operacji czyszczenia przestrzeni dyskowej, zostają wyczyszczone wszystkie elementy ze standardowej listy elementów umieszczonej w widoku File Sanitizer (patrz Procedury konfiguracji na stronie 41).

Operacje czyszczenia przestrzeni dyskowej można wykonać w jeden z poniższych sposobów:

1. Otwórz File Sanitizer (patrz Otwieranie narzędzia File Sanitizer na stronie 41), a następnie kliknij lub naciśnij **Bleach** (Wyczyść).
2. Gdy pojawi się okno dialogowe potwierdzenia, kliknij lub naciśnij **OK**.

— lub —

1. Kliknij prawym przyciskiem i przytrzymaj lub naciśnij i przytrzymaj ikonę **File Sanitizer** na pulpicie systemu Windows, a następnie kliknij **Wyczyść teraz**.
2. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij lub naciśnij **Bleach** (Wyczyść).

Przeglądanie plików dziennika

Za każdym razem, gdy wykonywana jest operacja niszczenia lub czyszczenia przestrzeni dyskowej, zostają wygenerowane pliki dziennika zawierające opis błędów lub czynności zakończonych niepowodzeniem. Pliki dziennika są aktualizowane zgodnie z wynikiem ostatniej operacji niszczenia lub czyszczenia przestrzeni dyskowej.

UWAGA: Pliki które zostały skutecznie zniszczone lub wyczyszczone nie są umieszczane w plikach dziennika.

Program generuje po jednym pliku dziennika dla operacji niszczenia i operacji czyszczenia przestrzeni dyskowej. Obydwa pliki dziennika są zapisywane na twardym dysku w następujących lokalizacjach:

- C:\Program Files\Hewlett-Packard\File Sanitizer**[Username]**_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer**[Username]**_DiskBleachLog.txt

W przypadku 64-bitowych wersji systemu Windows pliki dziennika znajdują się na dysku twardym w następujących lokalizacjach:

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer**[Username]**_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer**[Username]**_DiskBleachLog.txt

7 HP Device Access Manager (tylko wybrane modele)

Program HP Device Access Manager kontroluje dostęp do danych poprzez blokowanie dostępu do urządzeń przeznaczonych do transferu danych.

UWAGA: Niektóre interfejsy/urządzenia wejściowe, takie jak mysz, klawiatura, TouchPad czy czytnik linii papilarnych, nie są kontrolowane przez program Device Access Manager. Aby uzyskać więcej informacji, zobacz Nieobsługiwane klasy urządzeń na stronie 50.

Administratorzy systemu operacyjnego Windows® wykorzystują program HP Device Access Manager w celu kontrolowania dostępu do urządzeń systemowych oraz w celu ochrony przed nieuprawnionym dostępem:

- Profile dostępu do urządzeń są tworzone dla każdego użytkownika. Pozwalają one określić z których urządzeń dany użytkownik ma prawo korzystać, a które są dla niego niedostępne.
- Uwierzytelnianie Just In Time (JITA) umożliwia zdefiniowanym wcześniej użytkownikom dostęp poprzez uwierzytelnienie do urządzeń do których zwykle nie mają dostępu.
- Administratorzy i zaufani użytkownicy mogą uzyskać dostęp do urządzeń, do których dostęp blokuje program Device Access Manager przez dodanie ich do grupy administratorów urządzeń. Członkostwo w grupie jest zarządzane z poziomu ustawień zaawansowanych.
- Dostęp do urządzeni może zostać przyznany na podstawie przynależności od określonej grupy lub indywidualnie dla poszczególnych użytkowników.
- Dla urządzeń takich jak napędy CD-ROM i DVD, możliwość odczytu i zapisu można być przyznawana oddzielnie.

Program HP Device Access Manager jest konfigurowany automatycznie przy użyciu poniższych ustawień w trakcie działania kreatora konfiguracji programu HP Client Security.

- Uwierzytelnianie Just In Time Authentication (JITA) — Urządzenia przenośne są dostępne dla administratorów i użytkowników.
- Zasady kontroli dostępu do urządzenia pozwalają na pełny dostęp do innych urządzeń.

Uruchamianie programu Device Access Manager

1. Na ekranie startowym kliknij lub naciśnij ikonę aplikacji **HP Client Security** (Windows 8).

   — lub —

   Na pulpicie systemu Windows dwukrotnie kliknij lub naciśnij ikonę **HP Client Security** umieszczoną w obszarze powiadomień, z prawej strony paska zadań.

2. Na karcie **Device** (Urządzenie), kliknij lub naciśnij **Device Permissions** (Dostęp do urządzeń).

   - Zwykli użytkownicy mogą sprawdzić możliwość dostępu do poszczególnych urządzeń (patrz Widok użytkownika na stronie 48).
   - Administratorzy mają możliwość przeglądania i wprowadzania zmian w zakresie dostępu do urządzeń, skonfigurowanego na danym komputerze, klikając lub naciskając **Change** (Zmień) i wprowadzając hasło administratora (patrz Widok systemu na stronie 48).

Widok użytkownika

Po wybraniu **Device Permission** (Dostęp do urządzenia) zostaje wyświetlony widok użytkownika. W zależności od ustalonych zasad dostępu, zwykli użytkownicy i administratorzy mogą przeglądać swoje uprawnienia dostępu do poszczególnych klas urządzeń lub pojedynczych urządzeń na tym komputerze.

- **Current user** (Bieżący użytkownik) — Wyświetlana jest nazwa obecnie zalogowanego użytkownika.
- **Device Class** (Klasa urządzeń) — Wyświetlane są typy urządzeń.
- **Access** (Dostęp) — Wyświetlany jest status dostępu użytkownika do typów urządzeń oraz poszczególnych urządzeń.
- **Duration** (Okres dostępu) — Wyświetlany jest okres, w którym użytkownik ma dostęp do napędów CD/DVD-ROM lub dysków przenośnych.
- **Settings** (Ustawienia) — W obrębie tej karty Administratorzy mogą zdecydować, do których urządzeń dostęp będzie kontrolowany przez program Device Access Manager.

Widok systemu

Na karcie Widok systemu administratorzy mogą przyznać lub zablokować dostęp do urządzeń na tym komputerze grupie użytkowników lub grupie administratorów.

▲ Administratorzy uzyskują dostęp do karty Widok systemu poprzez kliknięcie lub naciśnięcie **Change** (Zmień), wprowadzenie hasła administratora i wybranie jednej z poniższych opcji:

- **Device Access Manager** — By włączyć lub wyłączyć program HP Device Access Manager z uwierzytelnieniem Just In Time Authentication, kliknij lub naciśnij **On** (Wł.) lub **Off** (Wył.).
- **Users and groups on this PC** (Użytkownicy i grupy na tym komputerze) — Wyświetla grupy użytkowników i administratorów, którym udostępniono lub zablokowano dostęp do wybranych klas urządzeń.
- **Device Class** (Klasa urządzeń) — Wyświetla klasy urządzeń i urządzenia, które są zainstalowane w systemie, lub mogły być wcześniej zainstalowane w systemie. By rozwinąć listę, kliknij ikonę **+**. Zostaną wyświetlone wszystkie urządzenia podłączone do komputera, a także przynależność poszczególnych grup administratorów i użytkowników. By odświeżyć widok listy, kliknij ikonę z okrągłą strzałką (Odśwież).
  - Ochroną jest zwykle objęta cała klasa urządzeń. Jeśli dostęp jest ustawiony na **Allow** (Zezwalaj), wybrany użytkownik lub grupa użytkowników posiada dostęp do wszystkich urządzeń w obrębie danej klasy.
  - Ochroną może być również objęte pojedyncze urządzenie.
  - Konfiguracja uwierzytelnienia Just In Time Authentication (JITA) pozwala wybranym użytkownikom na dostęp do napędów DVD/CD-ROM lub dysków przenośnych poprzez uwierzytelnienie. Aby uzyskać więcej informacji, zobacz Konfiguracja JITA na stronie 49.
  - Przyznawanie i blokada dostępu do innych klas urządzeń, takich jak przenośne nośniki pamięci (np. pamięć USB flash), porty szeregowe i równoległe, urządzenia Bluetooth®, modemy, czytniki PCMCIA/ExpressCard, urządzenia 1394, czytniki linii papilarnych i kart inteligentnych. W przypadku blokady dostępu do czytnika linii papilarnych i czytnika kart inteligentnych, mogą one być wykorzystane do wprowadzenia danych uwierzytelniających, lecz nie ma do nich dostępu podczas sesji roboczej komputera.

UWAGA: Jeśli do wprowadzenia danych uwierzytelniających są wykorzystywane urządzenia Bluetooth, dostęp do urządzenia Bluetooth nie powinien być ograniczony w zasadach zdefiniowanych w programie Device Access Manager.

- Gdy podczas wyboru ustawień na poziomie grupy lub klasy urządzeń, zostaniesz zapytany, czy ustawienia mają dotyczyć również obiektów podrzędnych, do wyboru masz dwie odpowiedzi:

  Yes (Tak) — Ustawienia zostaną wprowadzone również dla obiektów podrzędnych.

  No (Nie) — Ustawienia nie zostaną wprowadzone dla obiektów podrzędnych.

- Niektóre klasy urządzeń, jak np. napędy DVD lub CD-ROM, mogą być kontrolowane na późniejszym etapie poprzez blokadę lub przyznanie dostępu do odczytu lub zapisu.

UWAGA: Grupa Administratorów nie może zostać dodana do Listy użytkowników.

- **Access** (Dostęp) — Kliknij lub naciśnij strzałkę w dół, a następnie wybierz jeden z typów dostępu w celu przyznania lub zablokowania dostępu:
  - **Zezwalaj – Pełny dostęp**
  - **Zezwalaj – Tylko odczyt**
  - **Allow – JITA Required** (Zezwalaj – wymagane uwierzytelnienie JITA) — Aby uzyskać dodatkowe informacje, patrz Konfiguracja JITA na stronie 49.

    Jeśli zostanie wybrany ten rodzaj dostępu, na karcie **Duration** (Okres dostępu) kliknij lub naciśnij strzałkę w dół, aby wprowadzić limit czasowy dostępu.
  - **Odmów**
- **Duration** (Okres dostępu) — Kliknij lub naciśnij strzałkę w dół, aby wprowadzić limit czasowy dostępu do napędów CD/DVD-ROM lub dysków przenośnych (patrz Konfiguracja JITA na stronie 49).

Konfiguracja JITA

Konfiguracja uwierzytelnienia JITA pozwala administratorowi na przeglądanie i modyfikowanie list użytkowników i grup, którym przyznano dostęp do urządzeń na postawie uwierzytelnienia Just In Time Authentication (JITA).

Użytkownicy, którym przyznano dostęp na podstawie JITA uzyskują dostęp do niektórych urządzeń, do których zgodnie z ustawieniami programu **Device Class Configuration** mają ograniczony dostęp.

Dostęp na podstawie JITA może zostać przyznany na ustalony, liczony w minutach okres czasu lub na czas nieograniczony. Użytkownicy, którym przyznano dostęp na czas nieograniczony uzyskują dostęp od momentu przyznania, aż do chwili wylogowania z systemu.

Jeśli użytkownik uzyskuje dostęp JITA na czas ograniczony, na minutę przed końcem okresu JITA zostanie zapytany, czy chce przedłużyć czas dostępu. Natychmiast po wylogowaniu z systemu lub po zalogowaniu się innego użytkownika, okres dostępu JITA wygasa. Przy kolejnym logowaniu i próbie uzyskania dostępu do urządzenia poprzez JITA na ekranie zostaje wyświetlony komunikat z żądaniem wprowadzenia danych uwierzytelniających.

Uwierzytelnienie JITA jest dostępne dla następujących klas urządzeń:

- napędy DVD/CD-ROM
- dyski przenośne

Tworzenie zasad dostępu JITA dla użytkownika lub grupy użytkowników

Administrator może przyznać dostęp do określonych urządzeń użytkownikom lub grupom użytkowników wykorzystując uwierzytelnianie Just In Time Authentication (JITA).

1. Uruchom program **Device Access Manager**, a następnie kliknij lub naciśnij **Change** (Zmień).
2. Wybierz użytkownika lub grupę użytkowników, a następnie na karcie **Access** (Dostęp) dla grupy **Removable Disk drives** (Dyski przenośne) lub **DVD/CD-ROM drives** (Napędy DVD/CD-ROM) kliknij lub naciśnij strzałkę w dół, a następnie wybierz **Allow – JITA Required** (Zezwalaj – wymagane uwierzytelnienie JITA).
3. Na karcie **Duration** (Okres dostępu) kliknij lub naciśnij strzałkę w dół, aby wybrać czas dostępu na podstawie JITA.

Aby nowe ustawienia JITA zostały wprowadzone, użytkownik musi się wylogować i powtórnie zalogować.

Dezaktywacja dostępu JITA dla użytkownika lub grupy użytkowników

Administrator może dezaktywować dostęp przyznany użytkownikom lub grupom użytkowników na podstawie uwierzytelnienia JITA.

1. Uruchom program **Device Access Manager**, a następnie kliknij lub naciśnij **Change** (Zmień).
2. Wybierz użytkownika lub grupę użytkowników, a następnie na karcie **Access** (Dostęp) dla grupy **Removable Disk drives** (Dyski przenośne) lub **DVD/CD-ROM drives** (Napędy DVD/CD-ROM) kliknij lub naciśnij strzałkę w dół, a następnie wybierz **Deny** (Odmów).

Przy kolejnym logowaniu użytkownik nie uzyska dostępu do urządzenia.

Ustawienia

Widok **Settings** (Ustawienia) pozwala administratorom na przeglądanie i zmianę dysków, do których dostęp jest kontrolowany poprzez program Device Access Manager.

UWAGA: Program Device Access Manager musi być aktywny podczas konfiguracji listy liter dysków (patrz Widok systemu na stronie 48).

Nieobsługiwane klasy urządzeń

HP Device Access Manager nie obsługuje następujących klas urządzeń:

- Urządzenia wejściowe i wyjściowe
  - Napędy CD-ROM
  - Dysk
  - Kontroler napędu dyskietek (FDC)
  - Kontroler napędu twardego dysku (HDC)
  - Interfejsy HID
  - Interfejsy podczerwieni
  - mysz.
  - Złącze szeregowe wieloportowe
  - klawiatura

- Drukarki Plug and play (PnP)
- Drukarka
- Aktualizacja drukarki

- Przycisk
  - Zaawansowane zarządzanie zasilaniem (APM)
  - Bateria
- Różne
  - Komputer
  - Dekoder
  - Wyświetlacz
  - Zunifikowany sterownik wyświetlacza Intel®
  - Legacard
  - Sterownik multimediów
  - Zmieniacz nośnika
  - Technologia pamięci
  - Monitor
  - Urządzenia wielofunkcyjne
  - Net client
  - Net service
  - Net trans
  - Procesor
  - Adapter SCSI
  - Akcelerator bezpieczeństwa
  - Urządzenia bezpieczeństwa
  - System
  - Nieznane
  - Wolumin
  - Migawka woluminu

8 HP Trust Circle

HP Trust Circles to narzędzie służące do ochrony plików i dokumentów, które łączy możliwość szyfrowania plików z wygodną możliwością dzielenia dokumentów w ramach kręgu zaufania. Narzędzie szyfruje pliki przechowywane w określonych przez użytkownika folderach, chroniąc je przed dostępem osób spoza kręgu zaufania. Po zabezpieczeniu pliki mogą być wykorzystywane i współdzielone tylko przez członków kręgu. Jeśli chroniony plik otrzyma osoba spoza kręgu, pozostaje on zaszyfrowany i osoba ta nie uzyska do niego dostępu.

Uruchamianie narzędzia Trust Circles

1. Na ekranie startowym kliknij lub naciśnij ikonę aplikacji **HP Client Security**.

   — lub —

   Na pulpicie systemu Windows dwukrotnie kliknij lub naciśnij ikonę **HP Client Security** umieszczoną w obszarze powiadomień, z prawej strony paska zadań.

2. Na karcie **Data** (Dane), kliknij lub naciśnij **Trust Circles**.

Rozpoczęcie pracy

Istnieją dwa sposoby na wysyłanie zaproszeń (pocztą elektroniczną) i odpowiedzi na nie:

- **Using Microsoft® Outlook** (Za pomocą programu Microsoft® Outlook) — Poprzez użycie Trust Circles w programie Microsoft Outlook obsługa zaproszeń Trust Circle oraz odpowiedzi innych użytkowników Trust Circle zostaje zautomatyzowana.
- **Using Gmail, Yahoo, Outlook.com or other email services (SMTP)** (Za pomocą poczty elektronicznej Gmail, Yahoo, Outlook.com lub innych serwisów pocztowych (SMTP)) — Po wpisaniu imienia i nazwiska, adresu e-mail i hasła, program Trust Circles wykorzysta twoją usługę poczty e-mail do wysyłania wiadomości e-mail z zaproszeniem do osób wybranych do kręgu zaufania.

Aby skonfigurować profil podstawowy:

1. Wpisz imię i nazwisko oraz adres e-mail, a następnie kliknij lub naciśnij **Next** (Dalej).

   Imię i nazwisko staną się widoczne dla wszystkich członków zaproszonych do kręgu zaufania. Ten adres e-mail będzie używany do wysyłania i odbierania zaproszeń oraz rozsyłania odpowiedzi na zaproszenia.

2. Wpisz hasło dla konta e-mail, a następnie kliknij lub naciśnij **Next** (Dalej).

   Zostanie wysłana testowa wiadomość e-mail w celu potwierdzenia poprawności ustawień poczty e-mail.

   UWAGA: Komputer musi być wtedy podłączony do sieci.

3. W polu **Trust Circle Name** (Nazwa Trust Circle) wprowadź nazwę dla kręgu zaufania, a następnie kliknij lub naciśnij **Next** (Dalej).

4. Dodaj członków i foldery, a następnie kliknij lub naciśnij **Next** (Dalej). Krąg zaufania może zostać utworzony z jakimikolwiek wybranymi przez użytkownika folderami, natomiast zaproszenia do

kręgu mogą zostać wysłane pocztą e-mail do wszystkich wybranych członków. Jeśli z jakiegokolwiek powodu zaproszenie nie może zostać wysłane, na ekranie zostanie wyświetlone powiadomienie. Członkowie w każdej chwili mogą zostać zaproszeni ponownie do kręgu z poziomu widoku narzędzia Trust Circle poprzez kliknięcie **Your Trust Circles** (Twoje kręgi zaufania), a następnie podwójne kliknięcie lub naciśniecie kręgu zaufania. Aby uzyskać więcej informacji, zobacz Trust Circles na stronie 53.

Trust Circles

Można utworzyć krąg zaufania podczas procesu konfiguracji początkowej poprzez podanie swojego adresu e-mail, lub później w widoku narzędzia Trust Circle:

▲ W widoku narzędzia Trust Circle kliknij lub naciśnij **Create Trust Circle** (Utwórz krąg zaufania), a następnie wprowadź nazwę kręgu.

- By dodać członków do kręgu, kliknij lub naciśnij ikonę **M+**obok karty **Members** (Członkowie), a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
- By dodać członków do kręgu, kliknij lub naciśnij ikonę **M+**obok karty **Folders** (Foldery), a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Dodawanie folderów do kręgu zaufania

dodawanie folderów do nowego kręgu zaufania

- Podczas tworzenia kręgu zaufania można dodawać do niego foldery, klikając lub naciskając ikonę **+** obok karty **Folders** (Foldery), a następnie postępując zgodnie z instrukcjami wyświetlanymi na ekranie.

  — lub —

- Z poziomu Windows Explorer, kliknij prawym przyciskiem i przytrzymaj lub naciśnij i przytrzymaj folder, który nie stanowi jeszcze części kręgu zaufania, następnie wybierz kolejno **Trust Circle** (Krąg zaufania) i **Create Trust Circle from Folder** (Utwórz krąg zaufania z folderu).

WSKAZÓWKA: Możesz wybrać jeden lub więcej folderów.

Dodawanie folderów do istniejącego kręgu zaufania:

- W widoku narzędzia Trust Circle kliknij **Your Trust Circles** (Twoje kręgi zaufania), a następnie dwukrotnie kliknij lub naciśnij istniejący krąg zaufania, aby wyświetlić znajdujące się w nim foldery, kliknij lub naciśnij ikonę **+** obok karty **Folders** (Foldery), a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

  — lub —

- Z poziomu Windows Explorer, kliknij prawym przyciskiem i przytrzymaj lub naciśnij i przytrzymaj folder, który nie stanowi jeszcze części kręgu zaufania, następnie wybierz kolejno **Trust Circle** (Krąg zaufania) i **Add to existing Trust Circle from Folder** (Utwórz krąg zaufania z folderu).

WSKAZÓWKA: Możesz wybrać jeden lub więcej folderów.

Po dodaniu wybranego folderu do kręgu zaufania, narzędzie Trust Circles automatycznie szyfruje folder i jego zawartość. Po zaszyfrowaniu wszystkich plików na ekranie zostaje wyświetlony komunikat o zakończeniu szyfrowania. Dodatkowo, na wszystkich zaszyfrowanych ikonach folderów i plików jest wyświetlana zielona kłódka, sygnalizująca ich pełną ochronę.

Dodawanie członków do kręgu zaufania

Procedura dodawania nowych członków do kręgu zaufania obejmuje trzy czynności:

1. **Zaproszenie** — Najpierw właściciel kręgu zaufania zaprasza członka lub członków. Wiadomość e-mail z zaproszeniem może być rozesłana do wielu użytkowników lub zbiorczo do użytkowników z list/grup dystrybucyjnych.
2. **Akceptacja** — Zaproszona osoba odbiera zaproszenie i decyduje, czy je przyjąć, czy odrzucić. Jeśli zaproszona osoba przyjmie zaproszenie, do osoby zapraszającej zostaje wysłana wiadomość e-mail z informacją o przyjęciu zaproszenia. Jeśli zaproszenie zostaje wysłane do grupy, każdy z członków grupy otrzymuje zaproszenie osobno i ma prawo je przyjąć lub odrzucić .
3. **Rejestracja** — Zapraszający podejmuje ostateczną decyzję o tym, czy dodać członka do kręgu zaufania. Jeśli zapraszający zdecyduje się na zarejestrowanie nowego członka, do zapraszanej osoby jest wysyłana wiadomość e-mail z informacją potwierdzającą przyjęcie do kręgu. Opcjonalnie, osoba zapraszająca i zapraszana mogą zweryfikować bezpieczeństwo procesu zapraszania. Osobie zapraszanej zostaje wyświetlony kod weryfikujący, który musi podać zapraszającemu przez telefon. Po poprawnym zweryfikowaniu kodu, osoba zapraszająca może wysłać wiadomość e-mail z ostatecznym potwierdzeniem rejestracji.

Dodawanie członków do kręgu zaufania:

▲ Podczas tworzenia kręgu zaufania można dodawać do kręgu foldery, klikając lub naciskając ikonę **+** obok karty **Folders** (Foldery), a następnie postępując zgodnie z instrukcjami wyświetlanymi na ekranie.

- Jeśli korzystasz z programu Outlook, wybierz kontakty z książki adresowej programu Outlook, a następnie kliknij **OK**
- Jeśli korzystasz z innej usługi poczty e-mail, dodawaj nowe adresy e-mail ręcznie do narzędzia Trust Circle. Możesz je również wyszukać na liście adresów e-mail zarejestrowanych w Trust Circle.

Dodawanie członków do istniejącego kręgu zaufania:

▲ W widoku narzędzia Trust Circle kliknij **Your Trust Circles** (Twoje kręgi zaufania), a następnie dwukrotnie kliknij lub naciśnij istniejący krąg zaufania, aby wyświetlić znajdujące się w nim foldery, kliknij lub naciśnij ikonę **+** obok karty **Folders** (Foldery, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

- Jeśli korzystasz z programu Outlook, wybierz kontakty z książki adresowej programu Outlook, a następnie kliknij **OK**.
- Jeśli korzystasz z innej usługi poczty e-mail, dodawaj nowe adresy e-mail ręcznie do narzędzia Trust Circle. Możesz je również wyszukać na liście adresów e-mail zarejestrowanych w Trust Circle.

Dodawanie plików do kręgu zaufania

Do kręgu zaufania możesz dodawać pliki w jeden z poniższych sposobów:

- Skopiuj lub przenieś plik do folderu znajdującego się w istniejącym kręgu zaufania.

  — lub —

- Z poziomu eksploratora Windows kliknij prawym przyciskiem myszy lub naciśnij na plik, który nie jest zakodowany, wybierz **Krąg Zaufania**, a następnie wybierz **Szyfruj**. Zostaniesz poproszony o wybranie kręgu bezpieczeństwa, do którego powinien zostać dodany plik.

WSKAZÓWKA: Możesz wybrać jeden lub więcej plików.

Foldery zaszyfrowane

Wszyscy członkowie danego kręgu zaufania mogą przeglądać i edytować pliki należące do tego kręgu.

UWAGA: Trust Circle Manager/Reader nie synchronizuje plików między poszczególnymi członkami.

Pliki muszą być współdzielone za pomocą jednego z dostępnych sposobów, np. za pośrednictwem poczty e-mail, serwera ftp lub usług przechowywania w chmurze. Pliki skopiowane, przeniesione lub utworzone w folderze znajdującym się w kręgu bezpieczeństwa zostają natychmiast zabezpieczane.

Usuwanie folderów z kręgu zaufania

Usunięcie folderu z kręgu zaufania powoduje deszyfrowanie folderu i całej jego zawartości oraz usunięcie ich ochrony.

- W widoku narzędzia Trust Circle kliknij lub naciśnij**Your Trust Circles** (Twoje kręgi zaufania), dwukrotnie kliknij lub naciśnij istniejący krąg zaufania, aby wyświetlić znajdujące się w nim foldery, a następnie kliknij lub naciśnij ikonę**Trash can** (Kosz) obok folderu.

  — lub —

- Z poziomu Windows Explorer, kliknij prawym przyciskiem i przytrzymaj lub naciśnij i przytrzymaj folder, który stanowi części kręgu zaufania, a następnie wybierz kolejno **Trust Circle** (Krąg zaufania) i **Remove from trust circle** (Usuń z kręgu zaufania).

WSKAZÓWKA: Możesz wybrać jeden lub więcej folderów.

Usuwanie pliku z kręgu zaufania

Aby usunąć pliku z kręgu zaufania w eksploratorze Windows kliknij prawym przyciskiem myszy lub naciśnij i przytrzymaj plik, który nie jest zaszyfrowany, wybierz **Trust circle** (Krąg zaufania), a następnie wybierz **Deszyfruj plik**.

Usuwanie członków z kręgu zaufania

Nie można usunąć z kręgu zaufania w pełni zarejestrowanego członka. W takiej sytuacji należy utworzyć nowy krąg zaufania z wszystkimi pozostałymi członkami, przenieść wszystkie foldery i pliki do nowego kręgu, a następnie usunąć stary krąg. Dzięki temu wszelkie nowe pliki nie będą dostępne dla członka, który nie został dopuszczony do nowego kręgu, lecz będzie miał on dostęp do wszystkich plików współdzielonych wcześniej w ramach starego kręgu zaufania.

Jeśli członek nie jest w pełni zarejestrowany (otrzymał zaproszenie do kręgu zaufania lub nie zaakceptował zaproszenia do kręgu zaufania), można go usunąć w jeden z następujących sposobów:

- W widoku narzędzia Trust Circle kliknij lub naciśnij**Your Trust Circles** (Twoje kręgi zaufania), a następnie dwukrotnie kliknij lub naciśnij istniejący krąg zaufania, aby wyświetlić listę członków. Kliknij lub naciśnij ikonę **trash can** (Kosz) obok imienia i nazwiska członka, który ma zostać usunięty.
- W widoku narzędzia Trust Circle kliknij lub naciśnij **Members** (Członkowie), a następnie dwukrotnie kliknij lub naciśnij członka, aby wyświetlić wszystkie kręgi zaufania, w których posiada on członkostwo. Kliknij lub naciśnij ikonę **trash can** (Kosz) obok kręgu zaufania, aby usunąć członka.

Usuwanie kręgu zaufania

Krąg zaufania może zostać usunięty tylko przez jego właściciela.

▲ W widoku narzędzia Trust Circle kliknij lub naciśnij **Your Trust Circles** (Twoje kręgi zaufania), a następnie kliknij ikonę **trash bin** (Kosz) obok kręgu, który ma zostać usunięty.

Spowoduje to całkowite usunięcie kręgu zaufania ze strony oraz wysłanie do wszystkich jego członków wiadomości e-mail z informacją o usunięciu kręgu zaufania. Wszystkie pliki i foldery, które znajdowały się w kręgu zostaną zdeszyfrowane.

Ustawienia preferencji

W widoku narzędzia Trust Circle kliknij lub naciśnij **Preferences** (Preferencje). Wyświetlą się trzy karty

- **Ustawienia poczty e-mail**

Opcja	Opis
Nazwa użytkownika	Wyświetla nazwę obecnego użytkownika. By zmienić nazwę, wprowadź nową nazwę użytkownika. Zmiany są zapisywane automatycznie.
Adres poczty e-mail	Wyświetla obecnie używany adres e-mail. By zmienić adres, kliknij lub naciśnij **Change Email Settings** (Zmień ustawienia poczty e-mail), a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
Potwierdzanie nowych członków	Wybierz spośród poniższych opcji: ◦ **Confirm Automatically** (Potwierdzanie automatyczne) — Po otrzymaniu przyjęcia zaproszenia od zaproszonych osób, ich członkostwo w kręgu jest potwierdzane automatycznie, a do zaproszonych osób zostaje wysłany adres e-mail z potwierdzeniem członkostwa. ◦ **Confirm Manually** (Potwierdzanie ręczne) — Po otrzymaniu przyjęcia zaproszenia od zapraszanych osób, wymagane jest ręczne rejestrowanie członków w kręgu zaufania, a do zaproszonych osób zostaje wysłany adres e-mail z potwierdzeniem członkostwa. ◦ **Require Verification** (Żądanie weryfikacji) — Po otrzymaniu przyjęcia zaproszenia od zapraszanych osób, wymagany jest kod weryfikacji, aby zarejestrować zapraszane osoby. Właściciel kręgu musi skontaktować się z zapraszanymi osobami i poprosić o podanie kodu weryfikacji. Po podaniu poprawnego kodu weryfikacji zostają wysłane wiadomości e-mail z potwierdzeniem.
Uwierzytelnianie okresowe	Uwierzytelnianie okresowe wymaga od użytkownika wpisania hasła dostępu do systemu Windows po upływie określonego czasu (liczonego w minutach), a także podczas wykonywania operacji związanych z poufnością. Te ustawienia pozwalają użytkownikowi na włączenie i wyłączenie uwierzytelniania.
Limit czasowy uwierzytelnienia	Wybierz limit czasowy uwierzytelnienia (liczony w minutach), po upływie którego wymagane jest uwierzytelnienie.
Nie pokazuj komunikatów potwierdzeń	Zaznacz to pole wyboru, jeśli chcesz, aby komunikaty potwierdzeń nie były wyświetlane, lub odznacz, jeśli chcesz, aby były wyświetlane.
Chcę pomóc w poprawie jakości narzędzia HP Trust Circle poprzez anonimowe śledzenie użycia	Zaznacz to pole wyboru, jeśli chcesz uczestniczyć w programie poprawy jakości lub odznacz, jeśli nie chcesz w nim uczestniczyć.

- **Kopia zapasowa/Przywracanie**

Opcja	Opis
Tworzenie kopii zapasowych	Kopiuje dane aplikacji Trust Circle Manager/Reader (ustawienia i kręgi zaufania) do pliku kopii zapasowej. W przypadku awarii komputera lub systemu, plik ten może zostać wykorzystany do odtworzenia nowej instalacji narzędzia Trust Circles zgodnie z danymi zapisanymi w kopii zapasowej. **UWAGA:** W pliku zostają zapisane tylko dane związane tylko z narzędziem Trust Circle zainstalowanym na twoim komputerze (kręgi zaufania, ustawienia i członkowie). Dane z plików umieszczonych w folderach należących do kręgów zaufania nie są archiwizowane w kopii zapasowej. Kopie zapasowe tych plików należy wykonać oddzielnie. Aby wykonać kopię zapasową ustawień i danych użytkownika narzędzia Trust Circle: **1.** Kliknij lub naciśnij **Backup** (Kopia zapasowa). **2.** Wybierz nazwę pliku i katalog zapisu pliku kopii zapasowej, a następnie kliknij lub naciśnij **Save** (Zapisz). **3.** Wprowadź i potwierdź hasło, a następnie kliknij lub naciśnij **OK**. Hasło to będzie wymagane w celu odzyskania pliku.
Przywracanie	Przywracanie ustawień i kręgów zaufania z pliku kopii zapasowej, zwykle w przypadku awarii systemu lub migracji na inny komputer. Aby przywrócić ustawienia i dane użytkownika aplikacji Trust Circle Manager: **1.** Kliknij lub naciśnij **Restore** (Przywróć). **2.** Przejdź do katalogu i pliku kopii zapasowej, a następnie kliknij lub naciśnij **Open** (Otwórz). **3.** Wprowadź hasło, które zostało ustanowione podczas wykonywania kopii zapasowej.

- **About** (Informacje) — Wyświetla informacje o wersji programu Trust Circle Manager/Reader. Wyświetlane łącza pozwalają na pobranie aktualizacji programu Circle Manager do wersji Pro lub wyświetlenie zasad zachowania poufności firmy HP.

9 Odzyskiwanie sprzętu po kradzieży (tylko wybrane modele)

Usługa Computrace (do oddzielnego zakupu) umożliwia zdalne monitorowanie, zarządzanie i lokalizowanie komputera.

Po aktywacji, usługa Computrace jest konfigurowana zdalnie przez centrum obsługi firmy Absolute Software, będącej dostawcą usługi. Administrator w centrum obsługi klienta może skonfigurować usługę Computrace w sposób umożliwiający monitorowanie lub zarządzanie komputerem. Jeśli urządzenie zaginie lub zostanie skradzione, centrum obsługi klienta firmy Absolute Software pomaga lokalnym służbom w namierzeniu i odzyskaniu urządzenia. Po skonfigurowaniu, usługa Computrace pozostanie aktywna nawet po sformatowaniu lub wymianie twardego dysku.

Aby aktywować Computrace:

1. Podłączyć urządzenie do Internetu
2. Otworzyć aplikację HP Client Security Aby uzyskać więcej informacji, zobacz Uruchamianie programu HP Client Security na stronie 11.
3. Kliknij **Theft recovery** (Odzyskiwanie sprzętu po kradzieży).
4. Aby uruchomić kreatora aktywacji Computrace, kliknij **Pierwsze kroki**.
5. Wprowadź informacje kontaktowe oraz dane karty kredytowej lub wprowadź zakupiony wcześniej klucz produktu.

Kreator aktywacji doprowadzi transakcję do końca i utworzy twoje konto użytkownika na stronie centrum obsługi klienta Absolute Software. Po zakończeniu otrzymasz drogą e-mailową potwierdzenie z centrum obsługi klienta Absolute Software zawierające informacje o koncie.

Jeśli wcześniej był uruchamiany kreator aktywacji Computrace i konto w centrum obsługi klienta zostało już założone, możesz dokupić licencje dodatkowe kontaktując się z reprezentantem firmy HP.

Aby zalogować się do Centrum obsługi klienta:

1. Przejdź na stronę https://cc.absolute.com/.
2. W polu **Identyfikator logowania** i **Hasło** wprowadź dane uwierzytelniające, które otrzymałeś w e-mailu z potwierdzeniem, a następnie kliknij **Zaloguj**.

Z pomocą Centrum Obsługi Klienta możesz:

- Monitorować twoje komputery.
- Chronić dane na zdalnych komputerach.
- Zgłosić kradzież któregokolwiek z komputerów chronionych przez Computrance.

▲ Kliknij **Dowiedzieć się więcej**, by uzyskać dodatkowe informacje na temat Computrace.

10 Wyjątki dla lokalizowania haseł

Podczas uwierzytelnienia na etapie przedrozruchowym oraz na etapie uruchomienia programu HP Drive Encryption, wsparcie lokalizowania haseł jest ograniczone. Aby uzyskać więcej informacji, zobacz Edytory IME systemu Windows nie są obsługiwane podczas uwierzytelniania przedrozruchowego i z poziomu programu Drive Encryption. na stronie 59.

Co robić, gdy hasło zostanie odrzucone

Hasło może zostać odrzucone z następujących powodów:

- Użytkownik może korzystać z edytora IME, który nie jest obsługiwany. Jest to typowy problem w przypadku języków korzystających ze znaków dwubajtowych (koreański, japoński, chiński). Aby rozwiązać ten problem:

  1. W obszarze **Control Panel** (Panel sterowania) dodaj obsługiwany układ klawiatury (dodaj układ klawiatury US/English w obszarze Język chiński).
  2. Ustaw obsługiwaną klawiaturę jako domyślne urządzenie wejściowe.
  3. Uruchom program HP Client Security, a następnie wprowadź hasło systemu Windows.

- Użytkownik korzysta ze znaku, który nie jest obsługiwany. Aby rozwiązać ten problem:

  1. Zmień hasło dostępu do systemu Windows tak, aby zawierało jedynie obsługiwane znaki. Aby uzyskać dodatkowe informacje na temat nieobsługiwanych znaków, patrz Obsługa klawiszy specjalnych na stronie 60.
  2. Uruchom program HP Client Security, a następnie wprowadź hasło systemu Windows.

Edytory IME systemu Windows nie są obsługiwane podczas uwierzytelniania przedrozruchowego i z poziomu programu Drive Encryption.

W systemie Windows użytkownik może wybrać edytor IME (edytor metody wprowadzania znaków) w celu wprowadzania skomplikowanych znaków i symboli, jak na przykład znaki alfabetu japońskiego lub chińskiego, korzystając ze standardowej klawiatury ze znakami alfabetu rzymskiego.

Edytory IME nie są obsługiwane podczas uwierzytelniania przedrozruchowego i z poziomu programu Drive Encryption. Hasło do systemu Windows nie może być wprowadzone za pomocą edytora IME podczas uwierzytelniania przedrozruchowego i z poziomu programu Drive Encryption. Próby wprowadzenia hasła w taki sposób mogą doprowadzić do zablokowania komputera. W niektórych przypadkach Microsoft® Windows nie wyświetla IME, gdy użytkownik wprowadza hasło.

Rozwiązanie stanowi przejście na jeden z poniższych układów klawiatury, który przekłada się na układ klawiatury 00000411:

- Microsoft IME dla języka japońskiego
- Japoński układ klawiatury
- Office 2007 IME dla języka japońskiego — Gdy Microsoft lub strona trzecia używa terminu IME lub edytor metody wprowadzania znaków (input method editor), metoda wprowadzania może w

rzeczywistości nie być metodą IME. Powoduje to zamieszanie, lecz program odczytuje odwzorowanie kodu szesnastkowego. Dlatego też, jeśli znak IME jest mapowany do układu obsługiwanej klawiatury, program HP Client Security obsłuży taką konfigurację.

OSTRZEŻENIE! Jeśli program HP Client Security zostanie aktywowany, hasła wprowadzane za pomocą edytora Windows IME zostaną odrzucane.

Zmiana hasła za pomocą klawiatury o innym, lecz obsługiwanym układzie

Jeśli hasło jest wstępnie wprowadzone za pomocą klawiatury o danym układzie, na przykład U.S. English (409), a następnie użytkownik zmienia hasło, używając klawiatury o innym układzie, który jest również obsługiwany, np. Latin American (080A), zmienione hasło będzie działać w programie HP Drive Encryption, lecz nie zadziała na poziomie systemu BIOS, gdy użytkownik wykorzysta znaki z drugiego układu, które nie występują w układzie pierwszym (na przykład ē).

UWAGA: Administratorzy są w stanie rozwiązać ten problem z poziomu strony użytkownika programu HP Client Security (dostęp po kliknięciu ikony **Gear** (Ustawienia) na stronie głównej), usuwając użytkownika programu HP Client Security, a następnie wybierając żądany układ klawiatury w systemie operacyjnym i ponownie uruchamiając kreatora konfiguracji programu HP Client Security dla tego samego użytkownika. Żądany układ klawiatury będzie przechowywany w systemie BIOS, a hasła które mogą zostać wprowadzane za pomocą klawiatury tego układu będą odpowiednio ustawione w systemie BIOS.

Kolejny problem to użycie klawiatur o różnych układach, ale generujących te same znaki. Na przykład w przypadku układów klawiatury U.S. International (20409) i Latin American (080A) istnieje możliwość wpisania znaku é, lecz wymagane są do tego różne kombinacje klawiszy. Jeśli hasło zostało utworzone na klawiaturze o układzie Latin American, to układ klawiatury w systemie BIOS zostanie również ustawiony na Latin American, nawet jeśli hasło zostanie później zmienione za pomocą klawiatury o układzie U.S. International.

Obsługa klawiszy specjalnych

- chiński, słowacki, francuski (kanadyjski) i czeski

  Gdy użytkownik wybiera jeden z opisanych powyżej układów klawiatury i wprowadza hasło (na przykład abcdef), to hasło musi być wprowadzone przy jednocześnie wciśniętym klawiszu shift dla małych liter oraz shift icaps lock dla wielkich liter zawsze wtedy, gdy program HP Drive Encryption jest aktywny, a tryb uwierzytelnianie przedrozruchowego została załączony. Hasła składające się z cyfr należy wprowadzać za pomocą klawiatury numerycznej.

- koreański

  Gdy użytkownik wybiera jeden z opisanych powyżej układów klawiatury i wprowadza hasło (na przykład abcdef), to hasło musi być wprowadzone przy jednocześnie wciśniętym klawiszu prawy shift dla małych liter oraz prawy alt i caps lock dla wielkich liter zawsze wtedy, gdy program HP Drive Encryption jest aktywny, a tryb uwierzytelnianie przedrozruchowego została załączony.

- Nieobsługiwane znaki zostały wyszczególnione w poniższej tabeli:

Język	Windows	BIOS	Drive Encryption
arabski	Klawisze ﻷ ,ﻹ oraz ﻵ generują dwa znaki.	Klawisze ﻷ ,ﻹ oraz ﻵ generują jeden znak.	Klawisze ﻷ ,ﻹ oraz ﻵ generują jeden znak.

Język	Windows	BIOS	Drive Encryption
francuski (kanadyjski)	ç, è, à, i é z klawiszem caps lock generują w systemie Windows Ç, È, À, i É.	ç, è, à, i é z klawiszem caps lock generują podczas uwierzytelniania przedrozruchowego Ç, È, À, i É .	ç, è, à, i é z klawiszem caps lock generują w programie HP Drive Encryption Ç, È, À, i É.
hiszpański	układ 40a nie jest obsługiwany. Mimo to działa, gdyż program konwertuje go na układ c0a. Jednak ze względu na drobne różnice między tymi układami, zaleca się, aby użytkownicy hiszpańskojęzyczni zmienili układ klawiatury systemu Windows na 1040a (Spanish Variation) lub 080a (Latin American).	brak	brak
US international	◦ Klawisze ¡, ¤, ‘, ’, ¥ oraz × z górnego rzędu klawiatury będą odrzucane. ◦ Klawisze å, ® oraz Þ z drugiego rzędu klawiatury będą odrzucane. ◦ Klawisze á, ð oraz ø z trzeciego rzędu będą odrzucane. ◦ Klawisz æ z dolnego rzędu będzie odrzucany.	brak	brak
Czech	◦ Klawisz ğ będzie odrzucany. ◦ Klawisz į będzie odrzucany. ◦ Klawisz ų będzie odrzucany. ◦ Klawisze ė, ı oraz ż będą odrzucane. ◦ Klawisze ģ, ķ, ļ, ņ oraz ţ będą odrzucane.	brak	brak
słowacki	Klawisz ż będzie odrzucany.	◦ Klawisze š, ś oraz ş będą odrzucane podczas wpisywania z klawiatury, lecz można je będzie wprowadzić za pomocą klawiatury ekranowej. ◦ Martwy klawisz ţ generuje dwa znaki.	brak
Hungarian	Klawisz ż będzie odrzucany.	Klawisz ţ generuje dwa znaki.	brak

Język	Windows	BIOS	Drive Encryption
Slovenian	Klawisz żŻ będzie odrzucany w systemie Windows, natomiast klawisz ALT generuje klawisz martwy w systemie BIOS.	Klawisze ú, Ú, ů, Ů, ş, Ş, ś, Ś, š oraz Š będą odrzucane w systemie BIOS.	brak
japoński	Jeśli to możliwe, zaleca się stosowanie edytora IME programu Microsoft Office 2007. Mimo nazwy edytora IME, obsługiwany jest tak naprawdę układ klawiatury 411.	brak	brak

Glosariusz

Administrator
Patrz: **Administrator Windows**.

Administrator systemu Windows
Użytkownik mający pełne prawa do modyfikacji uprawnień dostępu i zarządzania innymi użytkownikami.

aktywacja
Zadanie, które musi być wykonane zanim będą dostępne jakiekolwiek funkcje narzędzia Drive Encryption. Administratorzy mogą aktywować narzędzie Drive Encryption z poziomu kreatora konfiguracji aplikacji HP Client Security lub z poziomu aplikacji HP Client Security. Proces aktywacji składa się z aktywacji oprogramowania, szyfrowania dysku i tworzenia początkowej kopii zapasowej klucza szyfrującego na przenośnym nośniku pamięci.

archiwum odzyskiwania awaryjnego
Bezpieczne miejsce, które pozwala na ponowne szyfrowanie kluczy głównego użytkownika pomiędzy kluczami kilku użytkowników systemu.

automatyczne niszczenie
Niszczenie zasobów zgodnie z harmonogramem zdefiniowanym w programie File Sanitizer.

Bluetooth
Technologia wykorzystująca radiową transmisję danych w celu zapewnienia komunikacji bezprzewodowej na niewielką odległość dla urządzeń wyposażonych w funkcję Bluetooth (komputerów, drukarek, myszy, telefonów komórkowych i innych).

czyszczenie przestrzeni dyskowej
Nadpisywanie usuniętych zasobów oraz przestrzeni nieużywanej danymi losowymi. Proces ten całkowicie kasuje usunięte już wcześniej dane, znacznie utrudniając ich odzyskanie.

dane uwierzytelniające
Informacje lub urządzenie fizyczne, które może zostać użyte do uwierzytelnienia pojedynczego użytkownika.

deszyfrowanie
Procedura kryptograficzna mająca na celu zamianę zaszyfrowanych danych w tekst.

domena
Grupa komputerów, które są częścią sieci i korzystają ze wspólnej bazy katalogów. Domen mają unikatowe nazwy, a każda z nich posiada zestaw wspólnych zasad i procedur.

Drive Encryption
Chroni dane poprzez zaszyfrowanie dysków, dzięki czemu informacje są niedostępne dla osób próbujących je odczytać bez odpowiedniego uwierzytelnienia.

DriveLock
Funkcja bezpieczeństwa parująca twardy dysk z użytkownikiem która wymaga wprowadzenie prawidłowego hasła DrivrLock podczas rozruchu komputera.

Folder kręgu zaufania
Jakikolwiek folder chroniony w ramach kręgu zaufania.

grupy
Grupa użytkowników, która posiada ten sam poziom dostępu lub braku dostępu do danej klasy urządzeń lub pojedynczych urządzeń.

HP SpareKey Recovery
Możliwość uzyskania dostępu do komputera poprzez podanie prawidłowej odpowiedzi na pytania bezpieczeństwa.

Jednokrotne logowanie
Funkcja, która przechowuje dane uwierzytelniające i umożliwia użycie HP Client Security w celu zapewnienia dostępu do aplikacji Windows i stron internetowych wymagających uwierzytelnienia.

karta bezstykowa
Plastikowa karta z zabudowanym układem scalonym, która może być użyta do uwierzytelnienia użytkownika.

karta ID
Gadżet na pulpicie systemowym Windows, służący do wizualnej identyfikacji twojego profilu poprzez wyświetlenie nazwy użytkownika i wybranego obrazka.

karta inteligentna
Urządzenie, które może być wykorzystywane wraz z kodem PIN do uwierzytelniania.

karta zbliżeniowa
Karta plastikowa z wbudowanym układem scalonym, która może być używana do uwierzytelniania wraz z innymi metodami w celu zwiększenia bezpieczeństwa.

klasa urządzeń
Wszystkie urządzenia należące do określonej grupy, jak na przykład dyski.

konto sieciowe
Konto administratora lub użytkownika systemu Windows na komputerze lokalnym, w grupie roboczej lub domenie.

Konto użytkownika systemu Windows
Użytkownik, który posiada uprawnienia do logowania się w sieci lub do indywidualnych komputerów.

kontrola dostępu do urządzenia
Lista urządzeń, do których dany użytkownik posiada dostęp lub do których odmówiono mu dostępu.

kopia zapasowa
Opcja kopii zapasowej umożliwia zapisanie ważnych danych programowych w pliku umieszczonym poza programem rodzimym. Plik kopii zapasowej może być w późniejszym okresie wykorzystany do odzyskania tych informacji na tym samym lub innym komputerze.

Krąg zaufania
Umożliwia łączenie wybranych danych w zdefiniowane grupy dostępu zaufanych użytkowników. Zapobiega to przypadkowemu lub celowemu dostawaniu się danych w niepowołane ręce. Dane zostają kryptograficznie powiązane z kręgiem zaufania dzięki technologii CryptoMill's Zero Overhead Key Management. Zapobiega to deszyfrowaniu dokumentów lub innych informacji poufnych przez użytkowników spoza kręgu zaufania

linie papilarne
Cyfrowe odwzorowanie linii papilarnych danego palca. Rzeczywisty obraz linii papilarnych nie jest przechowywany przez program HP Client Security.

logowanie
Obiekt w pakiecie oprogramowania HP Client Security w którego skład wchodzi nazwa użytkownika i hasło (oraz potencjalnie inne wybrane informacje), które mogą być wykorzystywane do logowania użytkownika na stronach internetowych i do aplikacji.

Metoda bezpiecznego logowania
Metoda wykorzystywana do zalogowania do komputera.

Niszczenie
Wykonanie algorytmu nadpisującego dane znajdujące się w zasobie za pomocą danych losowych.

Okno logowania Drive Encryption
Patrz: Przedrozruchowe uwierzytelnianie Drive Encryption.

PIN
Osobisty kod identyfikacyjny używany przez zarejestrowanych użytkowników do uwierzytelnienia.

PKI
Standard infrastruktury klucza publicznego (Public Key Infrastructure) definiujący interfejsy służące do tworzenia, zarządzania i używania certyfikatów i kluczy kryptograficznych.

podłączone urządzenie
Urządzenie podłączone do jednego z portów komputera.

ponowne uruchomienie
Proces ponownego uruchamiania komputera.

Przedrozruchowe uwierzytelnianie Drive Encryption
Ekran logowania pojawiający się przed uruchomieniem systemu Windows. Użytkownik musi wprowadzić nazwę użytkownika i hasło logowania do systemu Windows, numer PIN karty inteligentnej lub przyłożyć palec (ten, który został wcześniej zarejestrowany w systemie) do czytnika linii papilarnych. W przypadku wyboru logowania jednoetapowego, wprowadzenie prawidłowych informacji podczas logowania do narzędzia Drive Encryption pozwala na bezpośredni dostęp do systemu Windows, bez konieczności powtórnego logowania na ekranie logowania systemu Windows.

przywracanie
Proces, który kopiuje dane programowe z wykonanej wcześnie kopii zapasowej do danego programu.

ręczne niszczenie
Uruchamiany ręcznie proces natychmiastowego niszczenia wybranego zasobu lub zasobów, niezależny od zaplanowanych operacji czyszczenia automatycznego.

Strona główna
Lokalizacja centralna, z poziomu której można zarządzać funkcjami i ustawieniami programu HP Client Security.

System szyfrowania plików (EFS)
System, który szyfruje wszystkie pliki i podfoldery w wybranym folderze

szyfrowanie
Procedura, na przykład wykorzystująca algorytm szyfrujący, stosowany w kryptologii do zmiany zwykłego tekstu w tekst zaszyfrowany w celu niedopuszczenia do odczytania danych przez osoby nieuprawnione. Istnieje wiele typów szyfrowania danych i stanowią one podstawę szyfrowania w sieciach komputerowych. Często stosowane typy szyfrowania to Data Encryption Standard lub szyfrowanie za pomocą klucza publicznego.

szyfrowanie programowe
Użycie specjalnego oprogramowania do szyfrowania danych zapisanych na dysku twardym. Szyfrowanie odbywa się sektor po sektorze. Proces ten jest wolniejszy niż szyfrowanie sprzętowe

szyfrowanie sprzętowe
Użycie dysków samoszyfrujących zgodnych z wymogami OPAL Trusted Computing Group określającymi zasady zarządzania dyskami samoszyfrującymi, umożliwiające natychmiastowe szyfrowanie. Szyfrowanie sprzętowe jest bardzo szybkie i może trwać zaledwie kilka minut, podczas gdy szyfrowanie programowe może zająć nawet kilka godzin.

tożsamość
W programie HP Client Security oznacza grupę danych uwierzytelniających i ustawień, które są przetwarzane jako konto lub profil określonego użytkownika.

Trust Circle Manager/Reader

Trust Circle Reader akceptuje wyłącznie zaproszenia wysłane przez użytkowników programu Trust Circle Manager. Jednak Trust Circle Manager pozwala na tworzenie kręgów zaufania. Istnieje również możliwość zapraszania osób do kręgu zaufania za pomocą poczty e-mail oraz akceptowania zaproszeń od innych użytkowników. Po ustanowieniu kręgu zaufania, pliki zabezpieczone w kręgu mogą być bezpiecznie współdzielone przez wszystkich jego członków.

uwierzytelnianie
Proces weryfikacji tożsamości za pomocą danych uwierzytelniających, w tym hasła dostępu do systemu Windows, linii papilarnych, kart inteligentnych, kart bezstykowych lub zbliżeniowych.

uwierzytelnianie przedrozruchowe
Funkcja bezpieczeństwa wymagająca pewnej formy uwierzytelnienia, na przykład za pomocą karty inteligentnej, układu zabezpieczającego lub hasła w chwili, gdy komputer jest uruchamiany.

Uwierzytelnienie typu Just in Time
Patrz: Dokument pomocy programu HP Device Access Manager.

użytkownik
Dowolna osoba zapisana w aplikacji Drive Encryption. Użytkownicy bez praw administracyjnych posiadają ograniczone uprawnienia w Drive Encryption. Mogą tylko zapisywać własne sposoby uwierzytelniania (za zgodą administratora) i logować się.

Wbudowany układ zabezpieczający Trusted Platform Module (TPM)
Wbudowany układ zabezpieczający (TPM) służy raczej do uwierzytelniania komputera niż użytkownika. Uwierzytelnienie jest realizowane przez przechowywanie określonych danych na temat hosta, takich jak klucze kodujące, certyfikaty cyfrowe czy hasła. TPM zmniejsza ryzyko fizycznej kradzieży danych lub zdalnego ataku hakerskiego.

Windows Logon Security
Windows Logon Security (Zabezpieczenie logowania do systemu Windows) chroni twoje konto Windows, żądając określonych uwierzytelnień w celu uzyskania dostępu.

zasób
Składnik danych zawierający informacje osobiste lub pliki, dane historyczne lub związane z Internetem itd., znajdujące się na dysku twardym.

Indeks

A

aktywacja
  Drive Encryption dla standardowych dysków twardych 34
  Narzędzie Drive Encryption dla dysków samoszyfrujących 34

B

bezpieczeństwo 7
  cele kluczowe 6
  role 7

C

cele, bezpieczeństwo 6
czyszczenie przestrzeni dyskowej 43
  harmonogram 43
  ręczne 45
  uruchamianie 45

D

dane
  ograniczony dostęp do 6
dane logowania
  edytowanie 23
  importowanie i eksportowanie 26
  kategorie 24
  zarządzanie 24
dane uwierzytelniające logowania
  dodawanie 22
Dane uwierzytelniające pakietu HP Client Security 10
deszyfrowanie
  napędy 33
deszyfrowanie partycji dysków twardych 37
dezaktywacja narzędzia Drive Encryption 35
dodawanie członków 54
dodawanie folderów 53
dodawanie plików 54
dostęp
  blokowanie nieuprawnionego 6
  kontrola 47
Dostęp do programu Password Manager 20, 21
  łatwa konfiguracja 12
  Wyświetlanie i zarządzanie danymi uwierzytelniającymi 13

F

File Sanitizer 44
  procedury konfiguracji 41
  uruchamianie 41
foldery zaszyfrowane 55
FSA SecurID 20
funkcje, oprogramowanie HP Client Security 1
Funkcje oprogramowania HP Client Security 1

H

harmonogram niszczenia, ustawienia 42
hasło
  bezpieczne 8
  HP Client Security 8
  wskazówki 8
  zarządzanie 8
  zasady tworzenia 7
hasło logowania do systemu Windows 8
hasło odrzucone 59
hasło systemu Windows, zmiana 17
HP Client Security 14
  hasło do Backup and Recovery 8
HP Client Security, uruchamianie 11
HP Device Access Manager 47
  łatwa konfiguracja 13
  uruchamianie 47
HP Drive Encryption 33, 37
  aktywacja 34
  deszyfrowanie poszczególnych napędów 37
  dezaktywacja 34
  logowanie po aktywacji narzędzia Drive Encryption 34
  łatwa konfiguracja 13
  szyfrowanie poszczególnych napędów 37
  tworzenie kopii zapasowych i odzyskiwanie danych 38
  zarządzanie Drive Encryption 37
HP File Sanitizer 40
HP SpareKey 16
HP SpareKey Recovery 39
HP Trust Circle 52

I

ikona, użycie 44
Instrukcja prostej instalacji dla małych firm 12

K

karta inteligentna
  PIN 8
karty 18
klasy urządzeń, nieobsługiwane 50
kluczowe cele bezpieczeństwa 6
klucz szyfrowania
  tworzenie kopii zapasowej 38
konfiguracja
  klasa urządzeń 48
Konfiguracja JITA 49
Konfiguracja uwierzytelnienia Just In Time Authentication 49
kontrola dostępu do urządzenia 47
kradzież, ochrona przed 6

L

linie papilarne
  ustawienia administracyjne 15
  ustawienia użytkownika 16
linie papilarne, rejestracja 15
logowanie do komputera 35

M

Moje zasady 30

N

nieobsługiwane klasy urządzeń 50
nieuprawniony dostęp, blokowanie 6
niszczenie
  prawy przycisk 44
  ręczne 45
niszczenie za pomocą prawego przycisku 44

O

obsługa klawiszy specjalnych 60
ochrona zasobów przed zniszczeniem 43
odzyskiwanie dostępu za pomocą kluczy zapasowych 38
odzyskiwanie hasła 16
odzyskiwanie sprzętu po kradzieży 58
ograniczony
  dostęp do danych poufnych 6
  dostęp do urządzenia 47
Opcje zabezpieczeń 29
otwieranie narzędzia Drive Encryption 33

P

PIN 19
pliki dziennika, przeglądanie 45
preferencje 56
profil niszczenia 42
przeglądanie plików dziennika 45
przywracanie
  Dane uwierzytelniające pakietu HP Client Security 9

Q

Quick Links
  menu 23

R

ręczne uruchamianie operacji niszczenia 45
rozpoczęcie pracy 12, 52

S

siła hasła 25
szyfrowanie
  napędy 33
  oprogramowanie 34, 35, 37
  sprzęt 34, 35
szyfrowanie dysków twardych 36
szyfrowanie partycji dysków twardych 37
szyfrowanie programowe 34, 35, 37
szyfrowanie sprzętowe 34, 35

T

Trust Circles
  uruchamianie 52
tworzenie kopii zapasowej
  Dane uwierzytelniające pakietu HP Client Security 9
tworzenie kopii zapasowej klucza szyfrowania 38

U

uruchamianie
  File Sanitizer 41
  HP Device Access Manager 47
uruchamianie czyszczenia przestrzeni dyskowej 45
uruchamianie narzędzia Trust Circles 52
Urządzenia Bluetooth 17
usługa Computrace 58
ustawianie
  harmonogram czyszczenia przestrzeni dyskowej 43
  harmonogram niszczenia 42
ustawienia 16
  Dostęp do programu Password Manager 27
  HP SpareKey 16
  ikona 25
  PIN 20
  Urządzenia Bluetooth 17
ustawienia, karty zbliżeniowe, bezstykowe i inteligentne 19
ustawienia administracyjne
  linie papilarne 15, 16
Ustawienia zaawansowane 50
Ustawienia zaawansowane programu HP Client Security 28
usuwanie członków 55
usuwanie folderów 55
usuwanie kręgów zaufania 56
usuwanie plików 55

W

widok systemu 48
widok użytkownika 48
wyjątki dla haseł 59

Z

zapisywanie
  linie papilarne 15
zarządzanie
  hasła 20, 21
  szyfrowanie lub deszyfrowanie pojedynczych partycji dyskowych 37
zarządzanie dyskiem 37
zasady
  Administrator 28
  zwykły użytkownik 29
zasady JITA
  dezaktywacja dostępu dla użytkownika lub grupy użytkowników 50
  tworzenie zasad dla użytkownika lub grup użytkowników 50
zmiana hasła przy użyciu różnych układów klawiatur 60