HP ProtectTools
Instrukcja obsługi

Bluetooth jest znakiem towarowym należącym do jego właściciela i używanym przez firmę Hewlett-Packard Company w ramach licencji. Java jest znakiem towarowym w USA firmy Sun Microsystems, Inc. Microsoft i Windows są zarejestrowanymi w USA 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: Listopad 2009

Numer katalogowy dokumentu: 593308-241

Spis treści

1 Wprowadzenie do zabezpieczeń

Oprogramowanie HP ProtectTools Security Manager zapewnia funkcje zabezpieczeń pomagające chronić komputer, sieci i najważniejsze dane przez nieautoryzowanym dostępem. Zarządzanie oprogramowaniem HP ProtectTools Security Manager odbywa się poprzez Konsolę administracyjną.

Za pomocą konsoli administracyjnej HP ProtectTools lokalny administrator może przeprowadzać następujące zadania:

- Włączanie i wyłączanie funkcji zabezpieczeń
- Zapisywanie odcisków palców własnych i użytkowników tego komputera
- Zapisywanie scen dla identyfikacji twarzy
- Konfiguracja karty inteligentnej do uwierzytelniania
- Określenie wymaganych poświadczeń w celu uwierzytelniania
- Zarządzanie użytkownikami komputera
- Dostosowanie parametrów typowych dla urządzenia
- Konfiguracja zainstalowanych aplikacji Security Manager
- Dodawanie aplikacji Security Manager

Za pomocą panelu Security Manager, użytkownicy mogą przeprowadzać następujące zadania:

- Konfigurować opcje udostępnione przez administratora
- Zezwalać na ograniczoną kontrolę niektórych modułów HP ProtectTools

Moduły oprogramowania dostępne dla danego komputera mogą się różnić w zależności od modelu.

Moduły oprogramowania HP ProtectTools mogą być wstępnie instalowane, wstępnie ładowane lub dostępne do pobrania ze strony firmy HP. Więcej informacji znajdziesz na stronie http://www.hp.com.

UWAGA: Instrukcje w tym przewodniku napisano, zakładając, że na komputerze są już zainstalowane odpowiednie moduły oprogramowania HP ProtectTools.

Funkcje programu HP ProtectTools

Poniższa tabela wymienia kluczowe funkcje modułów HP ProtectTools.

Moduł	Podstawowe funkcje
HP ProtectTools Security Manager Administrative Console (dla administratorów)	• Konfiguracja poziomów zabezpieczeń i metody zabezpieczania logowania za pomocą Security Manager Setup Wizard. • Konfiguracja opcji ukrytych przed użytkownikami podstawowymi. • Dostęp użytkowników i konfiguracja Device Access Manager. • Dodawanie i kasowanie użytkowników HP ProtectTools oraz przeglądanie stanu uzytkowników za pomoca narzędzi administracyjnych.
HP ProtectTools Security Manager (dla użytkowników)	• Porządkowanie, konfigurowanie i zmiana nazw użytkowników i haseł. • Konfiguracja i zmiana danych logowania użytkowników, jak hasło Windows i Smart Card. • Konfiguracja i zmiana funkcji File Sanitizer Shred, Bleaching oraz ustawień. • Przeglądanie ustawień menedżera dostępu do urządzeń. • Konfiguracja preferencji oraz opcji Backup and Restore.
Credential Manager for HP ProtectTools (Password Manager)	• Zapisywanie, porządkowanie oraz ochrona nazw i haseł. • Konfiguracja ekranów logowania stron internetowych i programów, co zapewnia szybki i bezpieczny dostęp. • Zapisywanie nazwy użytkowników i haseł do stron internetowych w programie Password Manager. Przy kolejny wejściu na stronę, Password Manager wypełni odpowiednie pola i prześle automatycznie potrzebne informacje. • Tworzenie silniejszych haseł zapewniających lepsze bezpieczeństwo kont. Password Manager wypełnia i przesyła automatycznie potrzebne informacje.
Program Drive Encryption for HP ProtectTools (tylko w wybranych modelach)	• Zapewnia pełne szyfrowanie całych woluminów na dysku twardym. • Wymusza uwierzytelnianie przeduruchomieniowe w celu odszyfrowania i zapewnienia dostępu do danych.
Program Privacy Manager for HP ProtectTools (tylko w wybranych modelach)	• Wykorzystuje zaawansowane techniki logowania w celu weryfikacji źródła, integralności i bezpieczeństwa przy korzystaniu z poczty e-mail, dokumentów Microsoft® Office i komunikatorów internetowych (IM).

Moduł	Podstawowe funkcje
Program File Sanitizer for HP ProtectTools	• Pozwala na bezpieczne niszczenie danych cyfrowych (informacji poufnych, plików aplikacji, danych historycznych i pobieranych z Internetu itp.) znajdujących się w komputerze i okresowe oczyszczanie dysku twardego.
Program Device Access Manager for HP ProtectTools (tylko w wybranych modelach)	• Umożliwia menedżerom IT kontrolowanie dostępu do urządzeń w oparciu o profile użytkowników. • Uniemożliwia nieuprawnionym użytkownikom usuwanie danych za pomocą zewnętrznych nośników pamięci oraz wprowadzania wirusów do systemu za pomocą zewnętrznych nośników. • Umożliwia administratorom wyłączenie dostępu do nośników z możliwością zapisu dla wybranych osób lub grup.

Osiąganie podstawowych celów zabezpieczeń

Moduły programu HP ProtectTools współpracują, aby zapewnić rozwiązanie wielu kwestii dotyczących zabezpieczeń, w szczególności umożliwiają realizację następujących podstawowych celów zabezpieczeń:

- Zabezpieczenie przed celową kradzieżą
- Ograniczanie dostępu do cennych danych
- Zabezpieczenie przed nieuprawnionym dostępem z lokalizacji wewnętrznych i zewnętrznych
- Tworzenie zasad silnych haseł

Ochrona przed kradzieżą na zlecenie

Przykładem kradzieży na zlecenie jest kradzież komputera zawierającego tajne dane i informacje o klientach w trakcie kontroli bezpieczeństwa na lotnisku. Poniższe funkcje pomagają w ochronie przed kradzieżą na zlecenie:

- Funkcja uwierzytelniania przy uruchamianiu, jeśli jest włączona, zabezpiecza przed dostępem do systemu operacyjnego. Zobacz następujące procedury:
  - Security Manager
  - Drive Encryption

Ograniczenie dostępu do poufnych danych

Załóżmy, że zatrudniony przez firmę audytor pracuje w siedzibie i uzyskał dostęp do komputera w celu sprawdzenia danych finansowych. Nikt nie chce, by audytor był w stanie drukować pliki czy zapisywać je w urządzeniu takim jak nagrywarka CD. Poniższa funkcja pozwala na ograniczenie dostępu do danych:

- Device Access Manager for HP ProtectTools pozwala menedżerom IT na ograniczanie dostępu do urządzeń zapisujących, tak by poufne informacje nie mogły zostać wydrukowane lub skopiowane z dysku twardego na nośniki wymienne.

Zapobieganie nieautoryzowanemu dostępowi z lokalizacji wewnętrznych lub zewnętrznych

Nieautoryzowany dostęp do niezabezpieczonych komputerów firmowych stanowi namacalne ryzyko dla zasobów firmowych sieci takich jak informacje z usług finansowych, od zarządu, zespołu badawczo-rozwojowego i informacji prywatnych, takich jak kartoteki pacjentów czy osobiste zapisy finansowe. Poniższe funkcje pozwalają zapobiec nieautoryzowanemu dostępowi:

- Funkcja uwierzytelniania przy uruchamianiu, jeśli jest włączona, zabezpiecza przed dostępem do systemu operacyjnego. Zobacz następujące procedury:
  - Password Manager
  - Drive Encryption
- Program Password Manager pozwala na zabezpieczenie haseł czy dostępu do chronionych hasłem aplikacji przez nieautoryzowanych użytkowników.

- Device Access Manager for HP ProtectTools pozwala menedżerom IT na ograniczanie dostępu do urządzeń zapisujących, tak by poufne informacje nie mogły zostać skopiowane z dysku twardego.
- File Sanitizer umożliwia wykonywanie bezpiecznego kasowania danych przez niszczenie krytycznych plików i folderów oraz czyszczenia dysku twardego (przez nadpisywanie skasowanych danych, które nadal można odtworzyć).
- Funkcja DriveLock zabezpiecza przed dostępem do danych nawet wtedy, gdy dysk twardy zostanie wyjęty i zainstalowany w niezabezpieczonym systemie.

Tworzenie silnych reguł haseł

Jeśli zostanie wprowadzone zalecenie, by używać silnych haseł dla dziesiątek aplikacji internetowych i baz danych, program Security Manager zapewni zabezpieczony magazyn haseł i wygodę funkcji Single Sign On (Pojedyncze logowanie).

Dodatkowe elementy zabezpieczeń

Przypisywanie ról zabezpieczeń

Jedną z ważnych praktyk zarządzania zabezpieczeniami komputerów (szczególnie w dużych organizacjach) jest rozdzielenie obowiązków i praw między administratorów i użytkowników różnego typu.

UWAGA: W małej organizacji lub w przypadku komputera używanego do celów prywatnych jedna osoba może pełnić te wszystkie role.

W programie HP ProtectTools obowiązki i uprawnienia zabezpieczeń można podzielić między następujące role:

- Pracownik ds. zabezpieczeń — definiuje poziom zabezpieczeń dla firmy lub sieci i określa, które funkcje zabezpieczeń należy wdrożyć (np. karty Java™ Card, czytniki biometryczne czy tokeny USB).

  UWAGA: Wiele z funkcji HP ProtectTools może być dostosowanych przez osobę zarządzającą zabezpieczeniami we współpracy z firmą HP. Więcej informacji znajdziesz na stronie internetowej HP pod adresem http://www.hp.com.

- Administrator — stosuje funkcje zabezpieczeń zdefiniowane przez pracownika ds. zabezpieczeń i zarządza nimi. Może także włączać i wyłączać niektóre funkcje. Na przykład jeśli pracownik ds. zabezpieczeń podjął decyzję o wdrożeniu kart Java, administrator systemów informatycznych może włączyć tryb zabezpieczeń systemu BIOS z użyciem kart Java.

- Użytkownik — używa funkcji zabezpieczeń. Na przykład jeśli pracownik ds. zabezpieczeń i administrator systemów informatycznych włączyli w systemie obsługę kart Java, użytkownik może ustawić numer PIN karty Java i używać tej karty w celu uwierzytelniania.

OSTROŻNIE: Zachęca się administratorów do przestrzegania "najlepszych wzorców" w ograniczaniu uprawnień użytkowników końcowych i ograniczaniu dostępu dla użytkowników.

Nieautoryzowani użytkownicy nie powinni otrzymywać uprawnień administratora.

Zarządzanie hasłami programu HP ProtectTools

Większość funkcji programu HP ProtectTools Security Manager jest chroniona za pomocą haseł. W poniższej tabeli wymieniono powszechnie używane hasła, moduły oprogramowania, w których są ustawiane hasła, oraz funkcje haseł.

W tej tabeli wymieniono także hasła, które są ustawiane i używane tylko przez administratorów systemów informatycznych. Wszystkie inne hasła mogą być ustawiane przez zwykłych użytkowników i przez administratorów.

Hasło programu HP ProtectTools	Skonfiguruj następujący moduł	Funkcja
Hasło logowania do systemu Windows	Panel sterowania Windows® lub HP ProtectTools Security Manager	Można go używać do ręcznego logowania się oraz uwierzytelniania w celu uzyskania dostępu do niektórych funkcji Security Manager.

Hasło programu HP ProtectTools	Skonfiguruj następujący moduł	Funkcja
Hasło funkcji Tworzenie kopii zapasowych i przywracanie Security Manager	Security Manager, dla każdego użytkownika	Zabezpiecza dostęp do pliku Tworzenia kopii zapasowych i przywracania programu Security Manager.
Numer PIN karty Java™ Card	Java Card Security	Zabezpiecza dostęp do zawartości karty Java Card i uwierzytelnia użytkowników karty Java Card. Gdy numer PIN karty Java Card jest używany na potrzeby uwierzytelniania przy uruchamianiu, zabezpiecza również dostęp do programu narzędziowego Computer Setup i do zawartości komputera. Służy do uwierzytelnienia użytkowników funkcji szyfrowania dysku, jeśli wybrano token Java Card.

Tworzenie bezpiecznego hasła

Podczas tworzenia haseł należy najpierw dostosować się do specyfikacji ustawionych przez program. Jednak w ogólności należy wziąć pod uwagę następujące wskazówki pomagające w tworzeniu silnych haseł i zmniejszaniu ryzyka złamania hasła:

- Należy używać haseł składających się z więcej niż 6 znaków, a najlepiej z więcej niż 8.
- W haśle powinny znajdować się i wielkie, i małe litery.
- Zawsze, gdy jest to możliwe, w haśle należy umieścić znaki alfanumeryczne oraz znaki specjalne i interpunkcyjne.
- W haśle należy zastępować litery znakami specjalnymi lub cyframi. Na przykład cyfry 1 można używać zamiast liter I i L.
- Warto łączyć wyrazy z co najmniej dwóch języków.
- Należy rozdzielać wyraz lub frazę cyframi i znakami specjalnymi w środku, na przykład Maria2-2Kot45.
- Nie należy używać haseł, które można znaleźć w słowniku.
- Jako hasła nie należy używać nazwiska, imienia lub innych informacji osobistych, takich jak data urodzenia, imię zwierzęcia domowego lub nazwisko panieńskie matki, nawet jeśli będą pisane od tyłu.
- Hasła należy regularnie zmieniać. Można zmieniać tylko coraz większą część znaków.
- Zapisanego hasła nie wolno przechowywać w miejscu blisko komputera, w którym będzie widoczne.
- Hasła nie należy zapisywać w pliku na komputerze, takim jak wiadomość e-mail.
- Nie wolno udostępniać kont ani podawać swoich haseł innym osobom.

Wykonywanie kopii zapasowych i przywracanie poświadczeń HP ProtectTools

Za pomocą funkcji tworzenia kopii zapasowych i przywracania programu HP ProtectTools można wykonać kopię zapasową i przywrócić poświadczenia i ustawienia HP ProtectTools.

2 Rozpoczęcie pracy z kreatorem konfiguracji

Kreator konfiguracji HP ProtectTools przeprowadza przez konfigurację najczęściej używanych funkcji programu Security Manager. Wiele dodatkowych funkcji jest dostępne poprzez konsolę administracyjną HP ProtectTools. Te same ustawienia, które znajdują się w kreatorze oraz dodatkowe funkcje zabezpieczeń można konfigurować poprzez konsolę, która dostępna jest z menu Start systemu Windows®. Ustawienia te dotyczą komputera i wszystkich jego użytkowników.

1. Po tygodniu od początkowego skonfigurowania komputera po zalogowaniu lub wtedy, gdy użytkownik z uprawnieniami administratora po raz pierwszy przesunie palec po czytniku linii papilarnych, uruchomi się automatycznie Kreator konfiguracji Security Manager, aby przeprowadzić przez podstawowe kroki konfiguracji programu. Automatycznie zostanie uruchomiony przewodnik wideo dotyczący konfiguracji komputera.

   – lub –

   Uruchom HP ProtectTools Security Manager za pomocą ikony **gadżetu** na pasku bocznym Windows lub ikony w obszarze powiadomień z prawej strony paska zadań.

   

   Kolor paska górnego gadżetu informuje o różnych stanach:

   - Czerwona – HP ProtectTools nie został skonfigurowany lub wystąpił błąd w jednym z modułów ProtectTools.
   - Żółta – Sprawdź stronę stanów aplikacji (Applications Status) w Security Manager, aby sprawdzić, jakie trzeba wykonać zmiany w ustawieniach.
   - Niebieska – HP ProtectTools jest skonfigurowany i działa prawidłowo.

   UWAGA: Ikona gadżetu nie jest jest dostępna w systemie Windows XP.

   – lub –

Kliknij **Start**, **Wszystkie programy**, a następnie **HP ProtectTools Administrative Console**.

2. Przeczytaj ekran powitalny, a następnie kliknij przycisk **Next** (Dalej).

UWAGA: Na ekranie początkowym można wyłączyć ponowne uruchomienie kreatora przez wybranie jednej z opcji.

3. Kreator konfiguracji poprosi o potwierdzenie tożsamości.

   Wpisz hasło Windows lub zeskanuj linie papilarne czytnikiem, a następnie kliknij **Next** (Dalej).

   Jeśli nie jest dostępny czytnik linii papilarnych ani karta inteligentna, pojawi się prośba o podanie hasła Windows. Musisz użyć tego hasła w przyszłości, za każdym razem gdy wymagane jest uwierzytelnianie.

   Jeśli hasło Windows nie zostało jeszcze ustawione, zostanie wyświetlony monit o utworzenie hasła. Hasło Windows jest wymagane w celu ochrony konta Windows przed dostępem nieautoryzowanych osób, oraz w celu wykorzystania funkcji programu HP ProtectTools Security Manager.

4. Kreator konfiguracji przeprowadzi przez proces konfiguracji funkcji zabezpieczeń dotyczących wszystkich użytkowników komputera:

   - Windows Logon Security (Zabezpieczenie logowania systemu Windows) chroni kontoa Windows poprzez wymaganie określonych poświadczeń w celu uzyskania dostępu.
   - Drive Encryption (Szyfrowanie dysku) chroni dane poprzez zaszyfrowanie dysków, dzięki czemu informacje nie są czytelne dla osób nie posiadających właściwej autoryzacji.
   - Pre-Boot Security (Ochrona w trakcie uruchamiania) chroni komputer przed nieautoryzowanymi osobami zanim zostanie uruchomiony system Windows.

   UWAGA: Funkcja Pre-Boot Security nie jest dostępna, jeśli nie jest obsługiwana przez BIOS.

   W celu włączenia wybranej funkcji zabezpieczeń, zaznacz odpowiednie pole wyboru. Zaznaczenie większej ilości funkcji oznacza zwiększenie bezpieczeństwa komputera.

5. Na ostatniej stronie kreatora kliknij **Finish** (Zakończ).

   Zostanie wyświetlony panel Security Manager.

UWAGA: Jeśli nie zakończysz kreatora, zostanie uruchomiony automatycznie jeszcze dwa razy. Później dostęp do kreatora możliwy jest za pomocą okienka powiadamiającego znajdującego się w obszarze powiadamiania, po prawej stronie paska zadań (o ile nie zostało ono wyłączone), aż konfiguracja zostanie wykonana.

3 HP ProtectTools Security Manager Administrative Console

Zarządzanie oprogramowaniem HP ProtectTools Security Manager odbywa się poprzez Konsolę administracyjną.

UWAGA: Administracja programem HP ProtectTools wymaga uprawnień administratora.

Ta konsola zapewnia następujące funkcje:

- Włączanie i wyłączanie funkcji zabezpieczeń
- Zarządzanie użytkownikami komputera
- Dostosowanie parametrów typowych dla urządzenia
- Konfiguracja aplikacji Security Manager
- Dodawanie aplikacji Security Manager

▲ Aby skorzystać z aplikacji HP ProtectTools Security Manager, uruchom program HP ProtectTools Security Manager z menu Start lub kliknij prawym przyciskiem ikonę Security Manager w obszarze powiadomienia, znajdującym się z prawej strony paska zadań.

Konsola administracyjna HP ProtectTools i jej aplikacje dostępne są dla wszystkich użytkowników tego komputera.

Otwieranie konsoli administracyjnej

W przypadku zadań administracyjnych, takich jak ustawianie zasad systemowych, czy konfiguracja oprogramowania, otwórz konsolę w następujący sposób:

- Kliknij przycisk **Start**, **Wszystkie programy**, **HP**, a następnie **HP ProtectTools Administrative Console**.

  – lub –

  W lewym okienku programu Security Manager kliknij **Administration** (Administracja).

W przypadku zadań dotyczących użytkowników, takich jak rejestracja linii papilarnych, czy korzystanie z oprogramowania Security Manager, otwórz konsolę w następujący sposób:

- Kliknij **Start**, **Wszystkie programy**, kliknij **HP**, a następnie **HP ProtectTools Security Manager**.

  – lub –

  Kliknij dwukrotnie ikonę **HP ProtectTools Security Manager** w obszarze powiadomień z prawej strony paska zadań.

Korzystanie z konsoli administracyjnej

Konsola administracyjna Security Manager jest centralnym miejscem zarządzania funkcjami i aplikacjami programu HP ProtectTools Security Manager.

Konsola składa się z następujących elementów:

- **Tools** (Narzędzia)—Wyświetla poniższe kategorie służące konfiguracji zabezpieczeń w komputerze:
  - **Home** (Strona początkowa)—Umożliwia wybranie zadań zabezpieczających do wykonania.
  - **System**—Pozwala na konfigurację funkcji zabezpieczających i uwierzytelnianie użytkowników i urządzeń.
  - **Applications** (Aplikacje)—Wyświetla ogólne ustawienia programu HP ProtectTools Security Manager i aplikacji Security Manager.
  - **Data** (Dane)—Zawiera rozwijane menu łączy do aplikacji Security Manager chroniących dane.
- **Management Tools** (Narzędzia do zarządzania)—Zawiera informacje o dodatkowych narzędziach. Panel zawiera następujące opcje:
  - **HP ProtectTools Security Manager Setup Wizard** (Kreator konfiguracji HP ProtectTools Security Manager)—Przeprowadza przez konfigurację programu HP ProtectTools Security Manager.
  - **Help** (Pomoc)—Wyświetla niniejszy plik Pomocy, który zawiera informacje o programie Security Manager i zainstalowanych z nim aplikacjach. Pomoc dla aplikacji, które możesz dodać znajduje się wraz z tymi aplikacjami.
  - **About** (Informacje o programie)—Wyświetla informacje o programie HP ProtectTools Security Manager, takie jak numer wersji i informacje o prawach autorskich.
- **Main area** (Obszar główny)—Wyświetla ekran danej aplikacji.

4 Konfiguracja systemu

Grupa System dostępna jest w okienku menu Tools (Narzędzia) z lewej strony ekranu konsoli administracyjnej HP ProtectTools. Aplikacje w tej grupie możesz wykorzystać do zarządzania zasadami i ustawieniami dotyczącymi komputera, jego użytkowników i urządzeń.

Poniższe aplikacje znajdują się w grupie System:

- **Security** (Zabezpieczenia)—Zarządza funkcjami, uwierzytelnianiem i ustawieniami określającymi sposób, w jaki użytkownicy korzystają z komputera.
- **Users** (Użytkownicy)—Konfiguracja, zarządzanie i rejestracja użytkowników tego komputera.
- **Devices** (Urządzenia)—Zarządza ustawieniami dla urządzeń zabezpieczających które są wbudowane lub podłączone do komputera.

Konfiguracja uwierzytelniania dla komputera

W aplikacji uwierzytelnianie można wybrać, które funkcje zabezpieczeń powinny być zastosowane w tym komputerze, ustawić zasady związane z dostępem do komputera i skonfigurować inne ustawienia zaawansowane. Możesz określić poświadczenia wymagane do uwierzytelnienia każdej z klas użytkowników w trakcie logowania do Windows, lub logowania na stronach internetowych i do programów podczas sesji użytkownika.

Konfiguracja uwierzytelniania w komputerze:

1. W menu okienka Zabezpieczenia kliknij **Authentication** (Uwierzytelnianie).
2. Aby skonfigurować uwierzytelnianie w trakcie logowania, kliknij kartę **Logon Policy** (Zasady logowania), dokonaj zmian i kliknij **Apply** (Zastosuj).
3. Aby skonfigurować uwierzytelnianie sesji, kliknij kartę **Session Policy** (Zasady sesji), dokonaj zmian i kliknij **Apply** (Zastosuj).

Zasady logowania

Definiowanie zasad dotyczących poświadczeń wymaganych do uwierzytelnienia użytkownika w trakcie logowania do Windows:

1. W menu Tools (Narzędzia) kliknij **Security** (Zabezpieczenia), a następnie kliknij **Authentication** (Uwierzytelnianie).
2. Na karcie **Logon Policy** (Zasady logowania) kliknij kategorię użytkownika.
3. Określ poświadczenia uwierzytelniania wymagane dla wybranej kategorii użytkowników. Musisz określić co najmniej jedno poświadczenie.
4. Określ czy DOWOLNE (tylko jedno) z określonych poświadczeń jest wymagane, czy WSZYSTKIE z określonych poświadczeń są wymagane w celu uwierzytelnienia użytkownika Możesz także zabronić dowolnemu użytkownikowi dostępu do komputera.
5. Kliknij **Apply** (Zastosuj).

Zasady sesji

Definiowanie zasad dotyczących poświadczeń wymaganych do dostępu do aplikacji HP ProtectTools w trakcie logowania do Windows:

1. W menu Tools (Narzędzia) kliknij **Security** (Zabezpieczenia), a następnie kliknij **Authentication** (Uwierzytelnianie).
2. Na karcie **Session Policy** (Zasady sesji) kliknij kategorię użytkownika.
3. Określ poświadczenia uwierzytelniania wymagane dla wybranej kategorii użytkowników.
4. Określ czy wymagane jest tylko JEDNO z określonych poświadczeń, czy wymagane są WSZYSTKIE z określonych poświadczeń w celu uwierzytelnienia użytkownika. Możesz także nie wymagać poświadczeń w celu uzyskania dostępu do oprogramowania HP ProtectTools.
5. Kliknij **Apply** (Zastosuj).

Ustawienia

Możesz zezwolić na co najmniej jedno z następujących ustawień zabezpieczeń:

- **Allow One Step logon** (Zezwól na logowanie w jednym kroku)—Pozwala użytkownikom komputera na pominięcie logowania Windows jeśli uwierzytelnienie zostało wykonane na poziomie systemu BIOS czy zaszyfrowanego dysku.
- **Allow HP SpareKey authentication for Windows logon** (Zezwól na uwierzytelnianie HP SpareKey podczas logowania Windows)—Pozwala użytkownikom komputera na wykorzystanie funkcji HP SpareKey do logowania do Windows pomimo innych zasad uwierzytelniania wymaganych przez program Security Manager.

Edycja ustawień:

1. Kliknij by włączyć lub wyłączyć dane ustawienie.
2. Kliknij przycisk **Apply** (Zastosuj), aby zapisać dokonane zmiany.

Zarządzanie użytkownikami

W aplikacji Users (Użytkownicy) można monitorować i zarządzać użytkownikami HP ProtectTools w tym komputerze.

Wszyscy użytkownicy HP ProtectTools są wymieniani i weryfikowani zgodnie z zasadami ustawionymi w programie Security Manager oraz czy mają zarejestrowane odpowiednie poświadczenia umożliwiające spełnienie tych zasad.

W celu zarządzania użytkownikami, skorzystaj z następujących opcji:

- Aby dodać dodatkowych użytkowników, kliknij **Add** (Dodaj).
- Aby usunąć użytkownika, kliknij go i kliknij **Delete** (Usuń).
- Aby zapisać odciski palców lub dodać dodatkowe poświadczenia dla użytkownika, kliknij na nim i wybierz **Enroll** (Zapisz).
- Aby sprawdzić zasady dla danego użytkownika, kliknij na nim i przejrzyj zasady w dolnym oknie.

Określanie ustawień urządzenia

W aplikacji Device (Urządzenie) możesz ustalić ustawienia dostępne dla dowolnego wbudowanego lub podłączonego urządzenia zabezpieczającego rozpoznanego przez program HP ProtectTools Security Manager.

Odciski palców

Strona Fingerprints (Odciski palców) zawiera trzy karty: Enrollment (Zapisywanie), Sensitivity (Czułość), oraz Advanced (Zaawansowane).

Enrollment (Zapisywanie)

Możesz wybrać minimalną i maksymalną liczbę odcisków, które wolno zapisać użytkownikowi.

Możesz także usunąć wszystkie dane z czytnika linii papilarnych.

△ **OSTROŻNIE:** Skasowanie wszystkich danych z czytnika odcisków palców powoduje skasowanie tych informacji dla wszystkich użytkowników, w tym także administratorów. Jeśli zasady logowania wymagają tylko odcisków palców, żaden z użytkowników nie będzie mógł zalogować się do komputera.

Sensitivity (Czułość)

Przesuń suwak w celu regulacji czułości czytnika linii papilarnych podczas skanowania odcisków.

Jeśli odcisk palca nie jest rozpoznawany w jednolity sposób, może być konieczne niższe ustawienie. Wyższe ustawienie zwiększa czułość na zmiany w skanowaniu odcisków palców i tym samym zmniejsza prawdopodobieństwo niewłaściwej akceptacji. Ustawienie na poziomie wyższym-średnim zapewnia najlepsze połączenie bezpieczeństwa i wygody.

Advanced (Zaawansowane)

Możesz tak skonfigurować czytnik linii papilarnych, by oszczędzał energię gdy komputer pracuje na baterii.

Karta inteligentna

Możesz tak skonfigurować komputer, by blokował się automatycznie po wyjęciu karty inteligentnej. Jednak komputer zostanie zablokowany tylko wtedy, gdy karta została wcześniej użyta jako poświadczenie uwierzytelniania w trakcie logowania do Windows. Wyjęcie karty inteligentnej, gdy karta nie została użyta do logowania do Windows nie spowoduje zablokowania komputera.

▲ Zaznacz pole wyboru by włączyć lub wyłączyć blokowanie komputera po wyjęciu karty inteligentnej.

Twarz

Poziom zabezpieczeń dla rozpoznawania twarzy można ustawić tak, aby wyważyć łatwość użytkowania i możliwość złamania zabezpieczeń komputera.

1. Kliknij przycisk **Start**, **Wszystkie programy**, **HP**, a następnie **HP ProtectTools Administrative Console**.
2. Kliknij **Devices** (Urządzenia), a następnie kliknij **Face** (Twarz).

3. Większą wygodę zapewnia przesunięcie suwaka w lewo, a większą dokładność uzyskuje się przez przesunięcie suwaka w prawo.

   - **Convenience** (Wygoda)—Aby ułatwić zapisanym użytkownikom zalogowanie się w nietypowych sytuacjach, przesuń suwak w kierunku pozycji **Convenience** (Wygoda).
   - **Balance** (Zrównoważony)—Aby uzyskać kompromis między bezpieczeństwem i wygodą użytkowania, a komputer znajduje się w miejscu, w którym mogą wystąpić próby nieautoryzowanego dostępu, przesuń suwak w kierunku pozycji **Balance** (Zrównoważony).
   - **Accuracy** (Dokładność)—Aby utrudnić użytkownikowi zalogowanie, gdy zapisane sceny lub bieżące oświetlenie są odmienne i zmniejszyć prawdopodobieństwo błędnego zalogowania, przesuń suwak w kierunku pozycji **Accuracy** (Dokładność).

UWAGA: Poziom bezpieczeństwa odnosi się do wszystkich użytkowników

4. Kliknij **Apply** (Zastosuj).

Ustawienia zaawansowane

1. Kliknij przycisk **Start**, **Wszystkie programy**, **HP**, a następnie **HP ProtectTools Administrative Console**.
2. Kliknij **Devices** (Urządzenia), a następnie kliknij **Face** (Twarz).
3. Kliknij **Advanced** (Zaawansowane).

   - **Nie wymagaj nazwy użytkownika przy logowaniu Windows.**
     - Zaznacz tę opcję, aby umożliwić logowanie do systemu Windows bez podawania nazwy użytkownika.
     - Wyłącz tę opcję, aby nazwa użytkownika była wymagana.
   - **Enforce the use of PIN for face logon** (Wymagaj użycia PIN przy logowaniu za pomocą twarzy)—Zaznacz tę opcję, aby każdy użytkownik musiał ustawić i korzystać z PINu (osobistego numeru identyfikacyjnego) przy logowaniu.
     - **Minimum length allowed for PIN** (Minimalna długość PIN)—Strzałka do góry zwiększa, a strzałka do dołu zmniejsza minimalną wymaganą długość PINu.
     - **Maximum length allowed for PIN** (Maksymalna długość PIN)—Strzałka do góry zwiększa, a strzałka do dołu zmniejsza maksymalną dozwoloną długość PINu.
     - **Maximum retries allowed for PIN** (Maksymalna dozwolona liczba prób PIN)—Strzałka do góry zwiększa, a strzałka do dołu zmniejsza maksymalną dozwoloną liczbę prób ponownego podania PINu.

4. Kliknij **OK**.

5 Konfiguracja aplikacji

Grupa Applications (Aplikacje) dostępna jest w okienku menu Security Applications (Aplikacje zabezpieczające) z lewej strony konsoli administracyjnej HP ProtectTools. Możesz skorzystać z opcji Settings (Ustawienia), by dostosować zachowanie obecnie zainstalowanych aplikacji programu HP ProtectTools Security Manager.

Edycja ustawień aplikacji:

1. W menu Tools (Narzędzia), w grupie **Applications** (Aplikacje) kliknij **Settings** (Ustawienia).
2. Kliknij by włączyć lub wyłączyć dane ustawienie.
3. Kliknij przycisk **Apply** (Zastosuj), aby zapisać dokonane zmiany.

Karta General (Ogólne)

Następujące ustawienia dostępne są na karcie General:

- **Do not automatically launch the Setup Wizard for administrators** (Nie uruchamiaj automatycznie Kreatora instalacji dla administratorów)—Wybierz tę opcję by uniemożliwić kreatorowi na automatyczne uruchamianie po zalogowaniu.
- **Do not automatically launch the Getting Started wizard for users** (Nie uruchamiaj automatycznie kreatora Rozpoczęcie pracy dla użytkowników)—Wybierz tę opcję by uniemożliwić konfiguracji użytkownika na automatyczne uruchamianie po zalogowaniu.

Karta Applications (Aplikacje)

Wyświetlane tu ustawienia mogą ulec zmianie gdy nowe aplikacje zostaną dodane do programu Security Manager. Minimalne ustawienia pokazywane domyślnie to:

- **Applications status** (Stan aplikacji)—Włącza wyświetlanie stanu dla wszystkich aplikacji.
- **Password Manager**—Włącza aplikację Password Manager (Menedżer haseł) dla wszystkich użytkowników komputera.
- **Privacy Manager**—Włącza aplikację Privacy Manager (Menedżer prywatności) dla wszystkich użytkowników komputera.
- **Enable the Discover more button** (Włącz przycisk trybu odkrywania)—Pozwala wszystkim użytkownikom tego komputera na dodawanie aplikacji do HP ProtectTools Security Manager przez kliknięcie przycisku **[+] Discover more** (Tryb odkrywania).

Aby przywrócić ustawienia fabryczne wszystkich aplikacji, kliknij przycisk **Restore Defaults** (Przywróć domyślne).

6 Narzędzia do zarządzania

Dodatkowe aplikacji mogą być dostępne w celu dodania nowych narzędzi do zarządzania do programu Security Manager. Administrator tego komputera może wyłączyć tę funkcję poprzez aplikację Settings (Ustawienia).

Aby dodać dodatkowe narzędzia do zarządzania, kliknij **[+] Management tools** ([+] Narzędzia do zarządzania).

Aktualizacje i komunikaty

Jeżeli dostępne jest połączenie z Internetem, możesz skorzystać ze strony internetowej DigitalPersona http://www.digitalpersona.com/, aby sprawdzić, czy nie ma nowych aplikacji lub ustawić automatyczne sprawdzanie aktualizacji.

1. Aby zamówić informacje na temat nowych aplikacji i aktualizacji, zaznacz pole wyboru obok **Keep me informed about new applications and updates** (Informuj mnie o nowych aplikacjach i aktualizacjach).
2. W celu zaplanowania aktualizacji automatycznych, wybierz liczbę dni.
3. W celu sprawdzenia aktualizacji, kliknij **Check Now** (Sprawdź teraz).

7 HP ProtectTools Security Manager

HP ProtectTools Security Manager pozwala na znaczne zwiększenie bezpieczeństwa komputera.

Możesz użyć zainstalowanych aplikacji programu Security Manager, a także dodatkowych aplikacji dostępnych do pobrania z Internetu:

- Zarządzanie loginem i hasłami
- Łatwa zmiana hasła systemu operacyjnego Windows®
- Ustawianie preferencji programu
- Korzystanie z odcisków palców w celu zwiększenia bezpieczeństwa i wygody
- Zapisywanie scen do uwierzytelniania
- Konfiguracja karty inteligentnej do uwierzytelniania
- Wykonywanie kopii zapasowych i danych programu
- Dodawanie dalszych aplikacji

Otwieranie programu HP ProtectTools Security Manager

Możesz otworzyć program HP ProtectTools Security Manager w następujący sposób:

- Kliknij **Start**, **Wszystkie programy**, kliknij **HP**, a następnie **HP ProtectTools Security Manager**.
- Kliknij dwukrotnie ikonę **HP ProtectTools** w obszarze powiadomień po prawej stronie paska zadań.
- Kliknij prawym przyciskiem ikonę **HP ProtectTools** i kliknij **Otwórz HP ProtectTools Security Manager** .
- Kliknij gadżet **Security Manager ID Card** (Identyfikator Security Manager) na pasku bocznym Windows.
- Naciśnij kombinację klawiszy skrótów ctrl+Windows+h aby otworzyć menu Security Manager Quick Links (Szybkie łącza Security Manager).

Korzystanie z panelu programu Security Manager

Panel programu Security Manager jest centralnym miejscem służącym do uzyskania łatwego dostępu do funkcji Security Manager, aplikacji i ustawień.

▲ W celu otwarcia konsoli programu Security Manager, kliknij **Start**, **Wszystkie programy**, kliknij **HP**, a następnie **HP ProtectTools Security Manager**.

Panel składa się z następujących elementów:

- **ID Card** (Identyfikator)—Wyświetla nazwę użytkownika Windows i wybrany obraz identyfikujące zalogowane konto użytkownika.
- **Security Applications** (Aplikacje zabezpieczające)—Wyświetla menu rozwijane z łączami do konfiguracji poniższych kategorii zabezpieczeń:
  - **Menedżer poświadczeń**
  - **My Data (Moje dane)**
- **Discover more** (Tryb odkrywania)—Otwiera stronę, na której można odnaleźć dodatkowe aplikacje zwiększające bezpieczeństwo tożsamości, danych i komunikacji.
- **Main area** (Obszar główny)—Wyświetla ekran danej aplikacji.
- **Administration** (Administracja)—Otwiera konsolę administracyjną HP ProtectTools.
- **Przycisk Help** (Pomoc)—Wyświetla informacje o obecnym ekranie.
- **Advanced** (Zaawansowane)—Pozwala na dostęp do następujących opcji:
  - **Preferences** (Preferencje)—Pozwala na dostosowanie ustawień programu Security Manager.
  - **Backup and Restore** (Kopia zapasowa i odzyskiwanie)—Pozwala na wykonanie kopii zapasowej i odzyskanie danych.
  - **About** (Informacje)—Wyświetla informację o wersji Security Manager.

Procedury konfiguracji

Rejestrowanie poświadczeń

Strona Moja tożsamość służy do rejestrowania rozmaitych metod uwierzytelniania lub poświadczeń. Po zarejestrowaniu tych metod można ich używać w celu zalogowania się do programu Security Manager.

Zapisywanie odcisków palców

Jeśli komputer posiada wbudowany lub podłączony czytnik linii papilarnych, kreator konfiguracji HP ProtectTools przeprowadzi przez proces konfiguracji (zapisywania) odcisków palców.

1. Zostanie wyświetlony obrys dwóch dłoni. Zapisane palce zostaną zaznaczone na zielono. Kliknij palec na obrysie.

   UWAGA: Aby usunąć wcześniej zapisany odcisk palca, kliknij odpowiedni palec.

2. Po wybraniu palca do zapisania, pojawi się prośba o skanowanie tego palca, aż do jego prawidłowego zapisania. Zapisany palec zostanie zaznaczony na zielono na obrysie.

3. Musisz zapisać co najmniej dwa palce, najlepsze są palce wskazujące i środkowe. Powtórz kroki od 1 do 3 dla kolejnego palca.

4. Kliknij **Next** (Dalej), a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

UWAGA: Podczas zapisywania palców w ramach procesu Rozpoczęcie pracy, informacje o odciskach palców nie zostaną zapisane do czasu kliknięcia **Next** (Dalej). Jeśli zostawisz komputer na jakiś czas lub zamkniesz program, dokonane zmiany **nie** zostaną zapisane.

Zapisywanie scen

W celu korzystania z logowania za pomocą twarzy konieczne jest zapisanie jednej lub kilku scen.

Zapisywanie nowej sceny za pomocą kreatora konfiguracji HP ProtectTools Security Manager:

1. Kliknij dwukrotnie ikonę **HP ProtectTools Security Manager** na pasku bocznym z prawej strony ekranu.

2. Wpisz hasło Windows®, a następnie kliknij przycisk **Next** (Dalej).

3. Zaznacz pole wyboru **Enable security features** (Włącz funkcje zabezpieczeń), wybierz **Windows Logon Security** (Zabezpieczenie logowania systemu Windows), a następnie kliknij przycisk **Next** (Dalej).

4. Zaznacz pole wyboru **Choose your credentials** (Wybierz poświadczenia), wybierz **Face** (Twarz), a następnie kliknij **Next** (Dalej).

5. Kliknij **Enroll a new scene** (Zapisz nową scenę).

Po udanym zapisaniu sceny, można zapisać kolejne, jeżeli wystąpią problemy z logowania ze względu na zmianę jednego z następujących czynników:

- Od czasu ostatniego zapisywania twarz znacząco się zmieniła.
- Oświetlenie jest znacząco inne niż w przypadku poprzednich zapisów.
- W porównaniu z poprzednim zapisem na twarzy pojawiły się (lub zostały zdjęte) okulary.

UWAGA: Jeżeli masz problem z zapisaniem sceny, przysuń się bliżej do kamery. Tak jak w przypadku wszystkich zdjęć i nagrań wideo, bardzo istotne znaczenie ma oświetlenie oraz kontrast. Należy zadbać o to, aby oświetlona była przede wszystkim twarz, a nie tło. Jeżeli rozpoznawanie twarzy nie będzie w stanie dokonać uwierzytelnienia, warto spróbować ponownie zapisać scenę z poprawionym oświetleniem.

Zapisywanie nowej sceny za pomocą HP ProtectTools Security Manager:

1. Kliknij **Start**, **Wszystkie programy**, kliknij **HP**, a następnie **HP ProtectTools Security Manager**.
2. Kliknij **Credentials** (Poświadczenia), a następnie kliknij **Face** (Twarz).
3. Kliknij **Enroll a new scene** (Zapisz nową scenę).

Ustawienia zaawansowane użytkownika

1. Kliknij **Start**, **Wszystkie programy**, a następnie **HP ProtectTools Security Manager**.
2. Kliknij **Set up your authentication credentials** (Ustaw swoje poświadczenia), a następnie kliknij **Face** (Twarz).
3. Kliknij **Advanced** (Zaawansowane), a następnie skorzystaj z poniższych opcji.

   a. Jeżeli podczas logowania ma być wymagane użycie PINu, kliknij **Create PIN** (Utwórz PIN), wprowadź swoje hasło Windows, podaj nowy PIN, a następnie potwierdź podając go ponownie.

   b. W razie czego wybierz dodatkowe opcje. Następujące opcje dotyczą tylko bieżącego użytkownika:

   - **Play sound on face recognition events (Odtwórz dźwięk przy rozpoznawaniu twarzy)**
     - Zaznacz tę opcję, aby po przyjęciu (lub odrzuceniu) twarzy odtwarzany był dźwięk.
     - Wyłącz tę opcję, jeżeli nie chcesz z niej korzystać.
   - **Prompt to update scenes when logon fails (Zaproponuj uaktualnienie scen po nieudanym logowaniu)**
     - Zaznacz tę opcję, aby umożliwić użytkownikowi uaktualnienie sceny, gdy zalogowanie nie powiedzie się. Jeżeli weryfikacja przekroczy próg prawdopodobnego rozpoznania, użytkownik otrzyma możliwość dodania bieżącej sceny z nieudanego logowania tak, aby zwiększyć szanse zalogowania w przyszłości.
     - Wyłącz tę opcję, jeżeli nie chcesz z niej korzystać.
   - **Prompt to enroll a new scene when logon fails (Zaproponuj zapisanie nowej sceny po nieudanym logowaniu)**
     - Zaznacz tę opcję, aby umożliwić użytkownikowi dodanie nowej sceny, gdy zalogowanie nie powiedzie się, a weryfikacja nie przekroczy progu prawdopodobnego rozpoznania. Może to zwiększyć szanse zalogowania w przy następnej próbie.
     - Wyłącz tę opcję, jeżeli nie chcesz z niej korzystać.

   c. Aby zapisać nową scenę, kliknij przycisk **Enroll a new scene** (Zapisz nową scenę), a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Zmienianie hasła systemu Windows

Security Manager ułatwia i przyspiesz zmianę hasła Windows w porównaniu z panelem sterowania Windows.

Aby zmienić hasło Windows, wykonaj następujące kroki:

1. W panelu Security Manager kliknij **Credentials** (Poświadczenia), a następnie kliknij **Password** (Hasło).
2. Wpisz bieżące hasło w polu tekstowym **Current Windows password** (Obecne hasło Windows).

3. W polu **New Windows password** (Nowe hasło Windows) wpisz nowe hasło, a następnie wpisz je ponownie w polu **Confirm new password** (Potwierdź nowe hasło).

4. Kliknij **Change** (Zmień) by natychmiast zmienić obecne hasło na właśnie wprowadzone.

Konfiguracja karty inteligentnej

Jeśli wybierzesz opcję logowania za pomocą karty inteligentnej, a komputer posiada wbudowany lub podłączony czytnik kart inteligentnych, kreator konfiguracji Security Manager poprosi o ustawienie numeru PIN (osobisty numer identyfikacyjny) karty inteligentnej.

Ustawianie numeru PIN karty inteligentnej:

1. Na stronie **Set up smart card** (Konfiguruj kartę inteligentną) wprowadź i potwierdź numer PIN.

   Możesz także zmienić swój PIN. Podaj stary PIN, a następnie wprowadź nowy.

2. Aby kontynuować, kliknij **Next** (Dalej), a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

– lub –

▲ W panelu Security Manager kliknij **Credentials** (Poświadczenia), a następnie kliknij **Smart Card** (Karta inteligentna).

- Ustawianie numeru PIN karty inteligentnej—W **Set up smart card** (Konfiguruj kartę inteligentną) wprowadź i potwierdź numer PIN.
- Zmiana numeru PIN—Najpierw podaj stary PIN, a następnie wybierz nowy i potwierdź go.

Zadania ogólne

Aplikacje znajdujące się w tej grupie pomagają w zarządzaniu różnymi aspektami cyfrowej tożsamości.

- **Security Manager**—Tworzy i zarządza funkcją Quick Links (Szybkie łącza), co pozwala na uruchamianie i logowanie na stronach internetowych i programach za pomocą uwierzytelniania hasłem Windows, odciskiem palców, lub kartą inteligentną.
- **Credentials** (Poświadczenia)—Zapewnia sposób na łatwą zmianę hasła Windows, zapisanie odcisków palców lub skonfigurowanie karty inteligentnej.

Aby dodać więcej aplikacji, kliknij przycisk [+] **Discover more** (Tryb odkrywania) w dolnym lewym narożniku panelu. Przycisk ten może być wyłączony przez administratora.

Password Manager

Logowanie do Windows, stron internetowych i aplikacji jest łatwiejsze i bezpieczniejsze, gdy korzystasz z programu Password Manager. Możesz go użyć do tworzenia silniejszych haseł, których nie trzeba zapisywać czy zapamiętywać, a następnie łatwego i szybkiego zalogowania za pomocą odcisków palców, karty inteligentnej lub hasła Windows.

W programie Password Manager dostępne są następujące opcje:

- Dodaj, edytuj lub usuń loginy na karcie Manage (Zarządzaj).
- Użyj szybkich łączy by uruchomić domyślną przeglądarkę i zalogować się na dowolną stronę lub do programu, po ich skonfigurowaniu.
- Przeciągnij i upuść w celu uporządkowania szybkich łączy w kategorie.
- Szybko sprawdź, czy używane hasła nie są zagrożeniem bezpieczeństwa i automatycznie utwórz skomplikowane, silne hasła do użytku na nowych stronach.

Wiele funkcji programu Password Manager jest także dostępnych z ikony Password Manager wyświetlanej, gdy wyświetlany jest ekran logowania strony internetowej lub programu. Kliknij ikonę, by wyświetlić menu kontekstowe, gdzie możesz wybrać jedną z poniższych opcji.

Strony internetowe czy programy, do których login nie został jeszcze utworzony

Następujące opcje są widoczne w menu podręcznym:

- **Add [somedomain.com] to the Password Manager** (Dodaj [jakaśdomena.com] do Password Manager)—Pozwala na dodanie loginu do bieżącego ekranu logowania.
- **Open Password Manager** (Otwórz program Password Manager)—Uruchamia program Password Manager.
- **Icon settings** (Ustawienia ikon)—Pozwala na określenie warunków, w których wyświetlana jest ikona Password Manager.
- **Help** (Pomoc)—Wyświetla pomoc programu Password Manager.

Strony internetowe czy programy, do których login został już utworzony

Następujące opcje są widoczne w menu podręcznym:

- **Fill in logon data** (Uzupełnij dane logowania)—Umieszcza dane logowania w polach logowania i przesyła stronę (jeśli wybrano przesłanie podczas tworzenia lub ostatniej edycji loginu).
- **Edit logon** (Edytuj login)—Pozwala na edycję danych logowania dla tej strony internetowej.
- **Add a New Account** (Dodaj nowe konto)—Pozwala na dodanie konta do logowania.
- **Open Password Manager** (Otwórz program Password Manager)—Uruchamia aplikację Password Manager.
- **Help** (Pomoc)—Wyświetla pomoc programu Password Manager.

UWAGA: Administrator tego komputera może tak ustawić Security Manager, by wymagać co najmniej jednego poświadczenia podczas weryfikacji tożsamości.

Dodawanie loginów

Możesz łatwo dodać login do strony internetowej lub programu przez jednorazowe wprowadzenie informacji logowania. Od tego czasu Password Manager wprowadzi te informacje automatycznie. Możesz użyć tych loginów po przejściu na stronę internetową lub do programu, albo klikając login z menu **Logons** (Loginy), aby Password Manager otworzył stronę internetową lub program i zalogował się.

Dodawanie loginu:

1. Otwórz ekran logowania strony internetowej lub programu.
2. Kliknij strzałkę obok ikony **Password Manager**, a następnie kliknij jedną z poniższych opcji, zależnie od tego czy ekran logowania należy do strony lub programu:
   - W przypadku strony, kliknij **Add [domain name] to Password Manager** (Dodaj [nazwa domeny] do programu Password Manager).
   - W przypadku programu, kliknij **Add this logon screen to Password Manager** (Dodaj ten ekran logowania do programu Password Manager).
3. Wprowadź swoje dane logowania. Pola logowania na ekranie i odpowiadające im pola w oknie dialogowym są oznaczone grubą, pomarańczową ramką. Możesz także wyświetlić to okno dialogowe klikając opcję **Add Logon** (Dodaj login) z karty **Password Manager Manage** (Zarządzanie Password Manager). Niektóre opcje są zależne od urządzeń zabezpieczających podłączonych do komputera, na przykład za pomocą skrótu klawiaturowego ctrl+Windows+h, skanując odcisk palca, lub wkładając kartę inteligentną.
   a. W celu uzupełnienia pola logowania jednym z wcześniej sformatowanych wyborów, kliknij strzałki z prawej strony pola.
   b. W celu wyświetlenia haseł dla tego loginu, kliknij **Show password** (Pokaż hasło).
   c. W celu wypełnienia pól logowania, ale nie przesłania, odznacz pole wyboru **Automatically submit logon data** (Automatycznie prześlij dane logowania).
   d. Kliknij **OK**, po czym kliknij metodę uwierzytelniania, z której chcesz korzystać: **Fingerprints** (Odciski palców), **Password** (Hasło) lub **Face** (Twarz), a następnie zaloguj się za pomocą wybranej metody uwierzytelniania.

Znak plus zostanie usunięty z ikony Password Manager by poinformować, że utworzono login.

e. Jeżeli aplikacja Password Manager nie wykryje pól logowania, kliknij **More fields** (Więcej pól).

   i. Zaznacz pole obok każdego pola wymaganego przy logowaniu, lub odznacz pola, które nie są potrzebne przy logowaniu.

   ii. Jeżeli Password Manager nie może wykryć wszystkich pól logowania, pojawi się komunikat z prośbą o potwierdzenie kontynuowania. Kliknij **Yes** (Tak).

   iii. Pojawi się okno z wypełnionymi polami logowania. Kliknij po kolei ikonę każdego z pól i przeciągnij je do odpowiednich pól logowania, a następnie kliknij przycisk logowania na stronie.

   UWAGA: Po użyciu ręcznego trybu wprowadzania danych logowania dla danej strony, konieczne jest korzystanie z tej metody przy kolejnych logowaniach w przyszłości na tej samej stronie.

   UWAGA: Ręczny tryb wprowadzania danych logowania jest dostępny tylko w przeglądarce Internet Explorer 8.

   iv. Kliknij **Close** (Zamknij).

Za każdym razem, gdy wchodzisz na tę stronę lub otwierasz ten program, zostanie wyświetlona ikona Password Manager, wskazując że możesz skorzystać z zarejestrowanych poświadczeń w celu logowania.

Edycja loginów

Wykonaj następujące kroki, aby edytować login:

1. Otwórz ekran logowania strony internetowej lub programu.
2. Aby wyświetlić okno dialogowe, w którym można edytować informacje logowania, kliknij strzałkę obok ikony **Password Manager**, a następnie kliknij **Edit logon** (Edytuj login). Pola logowania na ekranie i odpowiadające im pola w oknie dialogowym są oznaczone grubą, pomarańczową ramką.

   Możesz także wyświetlić to okno dialogowe klikając opcję **Edit for the desired logon** (Edytuj wybrany login) z karty **Password Manager Manage** (Zarządzanie Password Manager).
3. Edytuj swoje informacje logowania.
   - W celu uzupełnienia pola logowania jednym z wcześniej sformatowanych wyborów, kliknij strzałki z prawej strony pola.
   - W celu dodania dodatkowych pól z ekranu do logowania, kliknij opcję **More fields** (Więcej pól).
   - W celu wypełnienia pól logowania, ale nie przesłania, odznacz pole wyboru **Submit logon data** (Prześlij dane logowania).
   - W celu wyświetlenia haseł dla tego loginu, kliknij **Show password** (Pokaż hasło).
4. Kliknij **OK**.

Korzystanie z menu Logons (loginy)

Password Manager zapewnia szybki i prosty sposób na uruchamianie stron internetowych i programów, dla których zostały utworzone loginy. Kliknij dwukrotnie login programu lub strony internetowej w menu

Logons (Loginy) lub karcie **Manage** (Zarządzaj) w **Password Manager**, aby otworzyć ekran logowania, a następnie wprowadź dane logowania.

Gdy utworzysz login, zostanie on automatycznie dodany do menu Password Manager Logons (Loginy Password Manager).

Wyświetlanie menu Logons:

1. Naciśnij skrót klawiszowy **Password Manager**. Ctrl+Windows+h jest ustawieniem fabrycznym. W celu zmiany skrótu klawiszowego, kliknij **Password Manager**, a następnie kliknij **Settings** (Ustawienia),
2. Zeskanuj swoje odciski palców (w komputerach z wbudowanym lub podłączonym czytnikiem linii papilarnych).

Organizowanie loginów w kategorie

Użyj kategorii by zachować porządek w loginach poprzez utworzenie co najmniej jednej kategorii. Następnie przeciągnij i upuść loginy do wybranych kategorii.

Dodawanie kategorii:

1. Na panelu Security Manager kliknij **Password Manager**.
2. Kliknij kartę **Manage** (Zarządzaj), a następnie kliknij **Add Category** (Dodaj kategorię).
3. Wprowadź nazwę kategorii.
4. Kliknij **OK**.

Dodawanie loginu do kategorii:

1. Umieść kursor nad wybranym loginem.
2. Naciśnij i przytrzymaj lewy przycisk myszy.
3. Przeciągnij login do listy kategorii. Kategorie zostaną podświetlone gdy przesuniesz nad nie mysz.
4. Zwolnij przycisk myszy, gdy zostanie podświetlona odpowiednia kategoria.

Loginy nie są przenoszone do kategorii, ale kopiowane do wybranej kategorii. Możesz dodać ten sam login do kilku kategorii, a także możesz wyświetlić wszystkie loginy klikając **All** (Wszystkie).

Zarządzanie loginami

Password Manager ułatwia zarządzanie informacją logowania dla nazw użytkowników, haseł i wielokrotnych kont logowania z jednego, centralnego miejsca.

Loginy są wymienione na karcie Manage (Zarządzaj). Jeśli utworzono wiele loginów dla tej samej strony, każdy z loginów jest wymieniony pod nazwą tej strony i jest przesunięty na liście loginów.

Zarządzenia loginami:

W panelu Security Manager kliknij **Password Manager**, a następnie kliknij kartę **Manage** (Zarządzaj).

- **Add a logon** (Dodaj login)—Kliknij **Add Logon** (Dodaj login), a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
- **Edit a logon** (Edytuj login)—Kliknij login, kliknij **Edit** (Edytuj), a następnie zmień dane logowania.
- **Delete a logon** (Usuń login)—Kliknij login, a następnie kliknij **Delete** (Usuń).

Dodawanie dodatkowego loginu do strony internetowej lub programu:

1. Otwórz ekran logowania strony internetowej lub programu.
2. Kliknij ikonę **Password manager** aby wyświetlić menu skrótów.
3. Kliknij **Add additional logon** (Dodaj dodatkowy login), a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Ocena siły hasła

Używanie silnych haseł do logowania na stronach internetowych i do programów jest istotnym aspektem ochrony swojej tożsamości.

Password Manager czyni monitorowanie i poprawę zabezpieczeń łatwiejszym dzięki natychmiastowej i automatycznej analizie siły każdego z haseł używanych do logowania na stronach internetowych i do programów.

Ustawienia ikony Password Manager

Password Manager próbuje rozpoznać ekrany logowania stron internetowych i programów. Gdy wykryje ekran logowania dla którego nie utworzono loginu, Password Manager poprosi o dodanie loginu do tego ekranu poprzez wyświetlenie ikony Password Manager ze znakiem "+".

Kliknij ikonę strzałki, a następnie kliknij **Icon Settings** (Ustawienia ikony) by dostosować sposób, w jaki **Password Manager** zarządza stronami logowania.

- **Prompt to add logons for logon screens** (Pytaj o dodanie loginów do ekranów logowania)—Kliknij tę opcję by Password Manager pytał, czy dodać login gdy zostanie wyświetlony ekran logowania, który nie posiada jeszcze skonfigurowanego loginu.
- **Exclude this screen** (Pomiń ten ekran)—Zaznacz te pole wyboru tak, by Password Manager nie pytał o dodanie loginu do tego ekranu logowania.

Dodatkowe ustawienia Security Manager dostępne są po kliknięciu **Password Manager**, a następnie kliknięciu **Settings** (Ustawienia) na panelu Password Manager.

Ustawienia

Możesz określić ustawienia dla dostosowania HP ProtectTools Security Manager:

1. **Prompt to add logons for logon screens** (Pytaj czy dodać loginy do ekranów logowania)—Ikona Password Manager ze znakiem plusa jest wyświetlana gdy zostanie wykryty ekran logowania strony internetowej lub programu, wskazując że możesz dodać login dla tego ekranu do zbioru haseł. W celu wyłączenia tej funkcji, w oknie dialogowym **Icon Settings** (Ustawienia ikony) odznacz pole obok opcji **Prompt to add logons for logon screens** (Pytaj czy dodać loginy do ekranów logowania).

2. **Open Password Manager with ctrl+Windows+H** (Otwórz Password Manager za pomocą ctrl+alt +H)—Domyślny skrót klawiaturowy dla menu Password Manager Quick Links to ctrl+Windows +H. W celu zmiany skrótu klawiszowego, kliknij tę opcję i wprowadź nowy skrót. Skróty mogą zwierać co najmniej jeden z następujących elementów: ctrl, alt lub shift i dowolny klawisz liter lub cyfr.

3. Kliknij **Apply** (Zastosuj), aby zapisać zmiany.

Poświadczenia

Poświadczenia Security Manager służą do sprawdzenia, czy jesteś tym za kogo się podajesz. Lokalni administratorzy tego komputera mogą ustawić, które poświadczenie mogą zostać użyte do udowodnienia tożsamości w trakcie logowania do konta Windows, stron internetowych lub programów.

Dostępne poświadczenia mogą być różne, zależnie od wbudowanych lub podłączonych do komputera urządzeń zabezpieczających. Każde obsługiwane poświadczenie będzie miało wpis w grupie **My Identity, Credentials** (Moja tożsamość, poświadczenia).

Dostępne poświadczenia, wymagania, oraz obecny stan są wymienione i mogą zawierać:

- Odciski palców
- Hasło
- Karta inteligentna
- Twarz

Aby zapisać lub zmienić poświadczenie, kliknij łącze, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Osobisty identyfikator

Identyfikator w jednoznaczny sposób określa właściciela tego konta Windows i zawiera jego nazwę i wybrany obraz. Jest na stałe wyświetlany w lewym górnym narożniku na stronach Security Manager i jako gadżet paska bocznego Windows.

Kliknięcie na Identyfikatorze na pasku bocznym jest jedną z metod na szybki dostęp do Security Manager.

Możesz zmienić obraz i sposób wyświetlania nazwy. Domyślnie wybrana jest nazwa użytkownika Windows i obraz wybrany w trakcie konfiguracji Windows.

Zmiana wyświetlanej nazwy:

1. W panelu Security Manager kliknij ikonę **ID Card** (Identyfikator) w lewym górnym rogu.
2. Kliknij pole z nazwą wprowadzoną dla konta w Windows. System wyświetli nazwę użytkownika Windows dla tego konta.
3. Aby zmienić nazwę, wpisz nową nazwę, a następnie kliknij przycisk **Save** (Zapisz).

Zmiana wyświetlanego obrazu:

1. W panelu Security Manager kliknij **ID Card** (Identyfikator) w lewym górnym rogu.
2. Kliknij przycisk **Choose picture** (Wybierz obraz), kliknij obraz, a następnie kliknij przycisk **Save** (Zapisz).

Ustawianie preferencji

Możesz dostosować ustawienia dla HP ProtectTools Security Manager. W panelu Security Manager kliknij **Advanced** (Zaawansowane), a następnie kliknij kartę **Preferences** (Preferencje). Dostępne ustawienia są wyświetlane na dwóch kartach: General (Ogólne) i Fingerprint (Odciski palców).

General (Ogólne)

Następujące ustawienia dostępne są na karcie General:

Appearance (Wygląd)—**Show icon on taskbar** (Pokaż ikonę na pasku zadań)

- Aby włączyć pokazywanie ikony na pasku zadań, zaznacz pole wyboru.
- Aby wyłączyć pokazywanie ikony na pasku zadań, odznacz pole wyboru.

Fingerprint (Odciski palców)

Następujące ustawienia dostępne są na karcie Fingerprint:

- **Quick Actions** (Szybkie akcje)—Użyj funkcji Quick Actions by wybrać zadanie Security Manager, które ma zostać wykonane podczas naciskania wybranego klawisza w trakcie skanowania odcisków palców.

  W celu przypisania szybkiej akcji do jednego z dostępnych klawiszy, kliknij opcję **(Key) + Fingerprint** (Klawisz+odcisk palca) po czym kliknij jedno z dostępnych zadań z menu.

- **Fingerprint Scan Feedback** (Reakcja na skanowanie odcisków)—Widoczne tylko wtedy, gdy dostępny jest czytnik linii papilarnych. Użyj tego ustawienia, by dostosować reakcję która następuje podczas skanowania odcisków palców.

  - **Enable sound feedback** (Włącz potwierdzenie dźwiękiem)—Security Manager reaguje dźwiękiem w trakcie skanowania odcisku palca, odtwarzając różne dźwięki dla odpowiednich zdarzeń w programie. Możesz przypisać nowe dźwięki do tych zdarzeń na karcie Dźwięki w Panelu sterowania Windows, lub wyłączyć je całkowicie przez odznaczenie tej opcji.

  - **Show scan quality feedback (Pokaż informację o jakości skanowania)**

    Aby wyświetlać informację o wszystkich skanowaniach niezależnie od jakości, zaznacz tę opcję.

    Aby wyświetlać informacje tylko o skanowaniach dobrej jakości, wyłącz tę opcję.

Wykonywanie kopii zapasowej i przywracanie danych

Zalecane jest regularne wykonanie kopii zapasowej danych programu Security Manager. Częstotliwość wykonywania kopii zależy od częstotliwości zmian w danych. Przykładowo, jeśli dodajesz nowe loginy codziennie, należy codziennie wykonywać kopię danych.

Kopie zapasowe mogą być także użyte do migracji z jednego komputera do drugiego. Nazywa się to importem i eksportem.

UWAGA: Ta funkcja kopiuje tylko dane.

HP ProtectTools Security Manager musi być zainstalowany w komputerze który ma otrzymać zapisane dane zanim dane będzie można odtworzyć z pliku kopii.

Wykonywanie kopii zapasowej danych:

1. W lewym okienku kliknij **Advanced** (Zaawansowane), a następnie kliknij **Backup and Restore** (Kopia zapasowa i odzyskiwanie).
2. Kliknij **Back up data** (Wykonaj kopię zapasową danych).
3. Zaznacz moduły, które chcesz umieścić w kopii zapasowej. W większości przypadków zaznacz wszystkie.
4. Wprowadź nazwę dla pliku. Domyślnie plik zostanie zapisany w folderze Dokumenty. Kliknij **Browse** (Przeglądaj) by wybrać inne miejsce.
5. Wprowadź hasło chroniące plik.
6. Sprawdź swoją tożsamość.
7. Kliknij przycisk **Finish** (Zakończ).

Odtwarzanie danych:

1. W lewym okienku kliknij **Advanced** (Zaawansowane), a następnie kliknij **Backup and Restore** (Kopia zapasowa i odzyskiwanie).
2. Kliknij **Restore data** (Przywróć dane).
3. Wybierz utworzony wcześniej plik magazynu. Możesz wprowadzić ścieżkę w polu lub kliknąć **Browse** (Przeglądaj).
4. Wprowadź hasło chroniące plik.
5. Zaznacz moduły, których dane chcesz odtworzyć. W większości przypadków dotyczy to wszystkich wymienionych modułów.
6. Kliknij przycisk **Finish** (Zakończ).

Discover more (Dowiedz się więcej)

Mogą być dostępne dodatkowe aplikacje, dodające nowe funkcje do tego programu.

Na panelu Security Manager kliknij **[+] Discover more** (Tryb odkrywania) by przejrzeć dodatkowe aplikacje.

UWAGA: Jeśli w lewej dolnej części panelu nie ma łącza **[+] Discover more** (Tryb odkrywania), został on wyłączony przez administratora tego komputera.

Aktualizacje i komunikaty

1. Aby zamówić informacje na temat nowych aplikacji i aktualizacji, zaznacz pole wyboru obok **Keep me informed about new applications and updates** (Informuj mnie o nowych aplikacjach i aktualizacjach).
2. W celu zaplanowania aktualizacji automatycznych, wybierz liczbę dni.
3. W celu sprawdzenia aktualizacji, kliknij **Check Now** (Sprawdź teraz).

Stan aplikacji zabezpieczających

Strona Security Manager Applications Status (Stan aplikacji Security Manager) podaje ogólny stan zainstalowanych aplikacji zabezpieczających. Wskazuje skonfigurowane aplikacje i stan konfiguracji każdej z nich. Strona podsumowania jest wyświetlana automatycznie, gdy otworzysz panel Security Manager lub gdy klikniesz **Check the status of the security applications** (Sprawdź stan zainstalowanych aplikacji zabezpieczających), **Security Applications** (Aplikacje zabezpieczające), albo **Check Now** (Sprawdź teraz) na ikonie **Gadget** (Gadżet) na pasku bocznym Windows po prawej stronie ekranu.

8 Drive Encryption for HP ProtectTools (tylko wybrane modele)

△ **OSTROŻNIE:** Jeśli zdecydujesz się usunąć moduł Drive Encryption, musisz wpierw odszyfrować wszystkie zaszyfrowane napędy. Jeśli tego nie zrobisz, nie będzie można uzyskać dostępu do danych na zaszyfrowanych napędach, chyba że zostały zarejestrowane w usłudze odzyskiwania szyfrowanych napędów. Ponowna instalacja modułu Drive Encryption nie umożliwi dostępu do zaszyfrowanych napędów.

Program Drive Encryption for HP ProtectTools (Szyfrowanie dysku) zapewnia całkowitą ochronę danych za pomocą szyfrowania dysku twardego w komputerze. Gdy funkcja Drive Encryption jest włączona, musisz zalogować się na ekranie logowania Drive Encryption, wyświetlanym przed uruchomieniem systemu Windows®.

Kreator konfiguracji HP ProtectTools pozwala administratorom Windows na włączenie funkcji Drive Encryption, wykonanie kopii zapasowej klucza szyfrującego, dodawanie i usuwanie użytkowników i wyłączenie funkcji Drive Encryption. Aby uzyskać więcej informacji, skorzystaj z pomocy oprogramowania HP ProtectTools Security Manager.

Poniższe zadania można przeprowadzić w programie Drive Encryption:

- Zarządzanie szyfrowaniem

  Szyfrowanie lub deszyfrowanie pojedynczych napędów

  UWAGA: Można zaszyfrować jedynie napędy wewnętrzne.

- Odzyskiwanie danych
  - Tworzenie kopii zapasowej kluczy
  - Odzyskiwanie

Procedury konfiguracji

Otwieranie programu Drive Encryption

1. Kliknij przycisk **Start**, **Wszystkie programy**, **HP**, a następnie **HP ProtectTools Administrative Console**.
2. W lewym okienku wybierz pozycję **Drive Encryption**.

Zadania ogólne

Uruchamianie programu Drive Encryption

Użyj Kreatora instalacji HP ProtectTools by aktywować Drive Encryption.

UWAGA: Kreator ten jest także używany do dodawania i usuwania użytkowników.

– lub –

1. Kliknij przycisk **Start**, **Wszystkie programy**, **HP**, a następnie **HP ProtectTools Administrative Console**.
2. W lewym okienku kliknij **Security** (Zabezpieczenia), a następnie **Features** (Funkcje).
3. Zaznacz pole wyboru **Drive Encryption**, a następnie kliknij przycisk **Next** (Dalej).
4. W opcji **Drives to be encrypted** (Napędy do zaszyfrowania), zaznacz pole wyboru dla dysku, który chcesz zaszyfrować.
5. Włóż urządzenie pamięci masowej do odpowiedniego gniazda.

   UWAGA: W celu zapisania klucza szyfrującego musisz użyć urządzenia USB w formacie FAT32.
6. W opcji **External storage device on which to save encryption key** (Urządzenie zewnętrzne do zapisania klucza szyfrującego), zaznacz pole wyboru obok urządzenia, na którym ma być zapisany klucz szyfrujący.
7. Kliknij **Apply** (Zastosuj).

   Rozpocznie się szyfrowanie dysku.

Aby uzyskać więcej informacji, skorzystaj z pomocy oprogramowania HP ProtectTools Security Manager.

Wyłączanie programu Drive Encryption

Użyj Kreatora instalacji HP ProtectTools by dezaktywować Drive Encryption. Aby uzyskać więcej informacji, skorzystaj z pomocy oprogramowania HP ProtectTools Security Manager.

– lub –

1. Kliknij przycisk **Start**, **Wszystkie programy**, **HP**, a następnie **HP ProtectTools Administrative Console**.
2. W lewym okienku kliknij **Security** (Zabezpieczenia), a następnie **Features** (Funkcje).
3. Odznacz pole wyboru **Drive Encryption**, a następnie kliknij **Apply** (Zastosuj).

   Rozpocznie się odszyfrowywanie dysku.

Logowanie po włączeniu Drive Encryption

Gdy włączysz komputer po aktywowaniu funkcji Drive Encryption i posiadasz odpowiednie konto użytkownika, musisz zalogować się na ekranie logowania Drive Encryption:

UWAGA: Jeśli administrator Windows włączył opcję Pre-boot Security (Zabezpieczenie przed uruchomieniem) w HP ProtectTools Security Manager, zalogujesz się do komputera natychmiast po jego włączeniu, a nie na ekranie logowania Drive Encryption.

1. Kliknij nazwę użytkownika i wpisz swoje hasło Windows lub numer PIN karty Java™ Card, albo odczytaj zarejestrowany palec.
2. Kliknij **OK**.

UWAGA: Jeśli korzystasz z klucza odzyskiwania do zalogowania się na ekranie logowania Drive Encryption, na ekranie logowania Windows będzie trzeba wprowadzić nazwę i hasło użytkownika Windows.

Ochrona danych za pomocą szyfrowania dysku twardego

Użyj Kreatora instalacji HP ProtectTools by chronić dane przez zaszyfrowanie dysku twardego:

1. W programie Security Manager, kliknij **Getting Started** (Rozpoczęcie pracy), a następnie kliknij ikonę **Security Manager Setup** (Konfiguracja Security Manager). Rozpocznie się demonstracja opisująca funkcje Security Manager. (Możesz także uruchomić program Security Manager na stronie Drive Encryption.)
2. W lewym okienku kliknij **Drive Encryption**, a następnie **Encryption Management** (Zarządzanie szyfrowaniem).
3. Kliknij **Change Encryption** (Zmień szyfrowanie).
4. Wybierz napęd lub napędy do zaszyfrowania.

UWAGA: Zdecydowanie zaleca się zaszyfrowanie dysku twardego.

Wyświetlanie stanu szyfrowania

Użytkownicy mogą wyświetlić stan szyfrowania w programie HP ProtectTools Security Manager.

UWAGA: Zmiany w stanie szyfrowania muszą być dokonywane w konsoli administracyjnej HP ProtectTools.

1. Otwórz **HP ProtectTools Security Manager**.
2. W opcji **My Data** (Moje dane) kliknij **Encryption Status** (Stan szyfrowania).

   Jeśli szyfrowanie dysku jest aktywne, stan dysku będzie opisany jednym z poniższych kodów stanu:

   - Active (Aktywny)
   - Inactive (Nieaktywny)
   - Not encrypted (Nie zaszyfrowany)
   - Encrypted (Zaszyfrowany)
   - Encrypting (Szyfrowanie)
   - Decrypting (Odszyfrowywanie)

Jeśli dysk twardy znajduje się w trakcie szyfrowania lub odszyfrowywania, pasek postępu wyświetla procentową wartość ukończenia procesu i pozostały czas do zakończenia szyfrowania lub odszyfrowywania.

Zadania zaawansowane

Zarządzanie programem Drive Encryption (zadanie administratora)

Strona Encryption Management (Zarządzanie szyfrowaniem) pozwala administratorom na przeglądanie i zmianę stanu Drive Encryption (włączanie i wyłączania) oraz na sprawdzanie stanu szyfrowania wszystkich dysków w komputerze.

- Jeśli stan to Inactive (Nieaktywny), szyfrowanie dysku nie zostało aktywowane w HP ProtectTools Security Manager przez administratora Windows i nie chroni dysku twardego. Użyj Kreatora instalacji HP ProtectTools Security Manager by aktywować Drive Encryption.
- Jeśli stan to Aktywny, szyfrowanie dysku zostało aktywowane i skonfigurowane. Dysk znajduje się w jednym ze stanów:
  - Not encrypted (Nie zaszyfrowany)
  - Encrypted (Zaszyfrowany)
  - Encrypting (Szyfrowanie)
  - Decrypting (Odszyfrowywanie)

Szyfrowanie lub deszyfrowanie pojedynczych napędów

W celu zaszyfrowania jednego lub kilku napędów w komputerze lub odszyfrowania napędu, który już został zaszyfrowany użyj funkcji Change Encryption (Zmień szyfrowanie):

1. Open **Konsolę administracyjną HP ProtectTools**, kliknij **Drive Encryption**, a następnie **Encryption Management** (Zarządzanie szyfrowaniem).
2. Kliknij **Change Encryption** (Zmień szyfrowanie).
3. W oknie dialogowym Change Encryption (Zmień szyfrowanie) zaznacz lub odznacz pole wyboru obok każdego z dysków twardych, które chcesz zaszyfrować lub odszyfrować, a następnie kliknij **OK**.

UWAGA: Jeśli dysk jest szyfrowany lub odszyfrowywany, pasek postępu wskazuje czas pozostały do zakończenia procesu w trakcie obecnej sesji. Jeśli komputer jest wyłączany lub rozpoczyna stan uśpienia, wstrzymania lub hibernacji w trakcie szyfrowania, a następnie jest ponownie uruchamiany, wskaźnik pozostałego czasu jest zerowany do początku, ale sam proces szyfrowania jest wznawiany w miejscu, w którym został zatrzymany. Pozostały czas i wskaźnik postępu będą zmieniać się szybciej by wskazać wcześniejszy postęp.

Kopia zapasowa i odzyskiwanie (zadanie administratora)

Strona Recovery (Odzyskiwanie) pozwala administratorom na wykonanie kopii zapasowej i odzyskiwanie kluczy szyfrujących.

Local Drive Encryption Key Backup (Kopia klucza szyfrującego napędy lokalne)—Pozwala na wykonanie kopii zapasowej klucza szyfrującego na przenośny napęd, jeśli Drive Encryption jest aktywne.

Tworzenie kopii zapasowej kluczy

Możesz wykonać kopię zapasową klucza szyfrującego dla zaszyfrowanego dysku na przenośnym urządzeniu pamięci masowej:

△ **OSTROŻNIE:** Pamiętaj, by przechowywać urządzenie zawierające kopię klucza w bezpiecznym miejscu, ponieważ jeśli zapomnisz hasła lub stracisz kartę Java Card, urządzenie to będzie jedyną metodą na uzyskanie dostępu do dysku twardego.

1. Open **Konsolę administracyjną HP ProtectTools**, kliknij **Drive Encryption**, a następnie **Recovery** (Odzyskiwanie).
2. Kliknij **Backup Keys** (Kopia zapasowa kluczy).
3. Na stronie Select Backup Disk (Wybierz dysk dla kopii zapasowej), zaznacz pole wyboru dla urządzenia, na którym ma być przechowywana kopia zapasowa klucza, a następnie kliknij przycisk **Next** (Dalej).
4. Przeczytaj informacje na następnej wyświetlonej stronie i kliknij **Next** (Dalej). Klucz szyfrujący zostanie zapisany na wybranym urządzeniu.
5. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij **Finish** (Zakończ).

Odzyskiwanie

Postępuj według poniższych kroków by dokonać odzyskiwania jeśli zapomnisz hasła:

1. Włącz komputer.
2. Włóż urządzenie przenośne zawierające kopię klucza.
3. Po wyświetleniu okna logowania Drive Encryption for HP ProtectTools, kliknij **Cancel** (Anuluj).
4. Kliknij **Options** (Opcje) znajdujące się w lewym dolnym rogu ekranu, a następnie kliknij **Recovery** (Odzyskiwanie).
5. Wybierz plik zawierający kopię klucza lub kliknij przycisk **Browse** (Przeglądaj), aby znaleźć tę lokalizację, a następnie kliknij przycisk **Next** (Dalej).
6. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij **OK**.

   Komputer zostanie uruchomiony.

UWAGA: Zdecydowanie zaleca się utworzenie nowego hasła po przeprowadzeniu odzyskiwania.

9 Program Privacy Manager for HP ProtectTools (tylko w wybranych modelach)

Program Privacy Manager for HP ProtectTools umożliwia wykorzystanie zaawansowanych technik logowania (uwierzytelniania) w celu weryfikacji źródła i bezpieczeństwa połączenia w trakcie korzystania z poczty e-mail, dokumentów Microsoft® Office i komunikatorów internetowych (IM).

Privacy Manager wykorzystuje infrastrukturę bezpieczeństwa zapewnianą przez HP ProtectTools Security Manager, zawierającą poniższe bezpieczne metody logowania:

- Uwierzytelnianie za pomocą odcisków palców
- Hasło systemu Windows®
- Karta Java™ Card dla HP ProtectTools

Możesz wykorzystać dowolną z powyższych metod bezpiecznego logowania w programie Privacy Manager.

Privacy Manager wymaga:

- HP ProtectTools Security Manager 5.00 lub nowszy
- System operacyjny Windows® 7, Windows Vista® lub Windows XP
- Microsoft Outlook 2007 lub Microsoft Outlook 2003
- Prawidłowe konto e-mail

UWAGA: Certyfikat Privacy Manager (certyfikat cyfrowy) musi zostać zamówiony i zainstalowany z programu Privacy Manager zanim będzie można skorzystać z funkcji zabezpieczających. Informacje na temat zamawiania certyfikatu Privacy Manager można znaleźć w części Zamawianie i instalacja Certyfikatu Privacy Manager na stronie 49.

Procedury konfiguracji

Otwieranie Privacy Manager

Otwieranie Privacy Manager:

1. Kliknij **Start**, **Wszystkie programy**, kliknij **HP**, a następnie **HP ProtectTools Security Manager**.
2. Kliknij opcję **Privacy Manager**.

– lub –

Prawym przyciskiem myszy kliknij ikonę **HP ProtectTools** w obszarze powiadomień po prawej stronie paska zadań, a następnie wybierz polecenie **Privacy Manager** (Menedżer prywatności) i kliknij **Configuration** (Konfiguracja).

– lub –

Na pasku narzędzi wiadomości e-mail programu Microsoft Outlook kliknij strzałkę w dół obok opcji **Send Securely** (Wyślij bezpiecznie), a następnie kliknij **Certificates** (Certyfikaty) lub **Trusted Contacts** (Zaufane kontakty).

– lub –

Na pasku narzędzi dokumentu Microsoft Office kliknij strzałkę w dół obok opcji **Sign and Encrypt** (Podpisz i zaszyfruj), a następnie kliknij **Certificates** (Certyfikaty) lub **Trusted Contacts** (Zaufane kontakty).

Zarządzanie certyfikatami programu Privacy Manager

Certyfikaty Privacy Manager chronią dane i wiadomości za pomocą technik kryptograficznych znanych jako infrastruktura klucza publicznego (PKI). PKI wymaga od użytkowników uzyskania kluczy kryptograficznych i certyfikatu Privacy Manager wystawionego przez zarządcę certyfikatów (CA). W przeciwieństwie do większości oprogramowania do deszyfrowania i uwierzytelniania wymagającego okresowego uwierzytelniania, Privacy Manager wymaga uwierzytelniania za każdym razem, gdy podpisujesz wiadomość e-mail lub dokument Microsoft Office za pomocą klucza kryptograficznego. Privacy Manager czyni bezpiecznym proces zapisywania i wysyłania ważnych informacji.

Możesz wykonać następujące zadania:

- Zamówić i zainstalować Certyfikat Privacy Manager
- Sprawdzić informacje szczegółowe Certyfikatu Privacy Manager
- Odnowić Certyfikaty Privacy Manager
- Gdy dostępne jest wiele certyfikatów, ustawić domyślny Certyfikat Privacy Manager używany przez Privacy Manager
- Usunąć i unieważnić Certyfikat Privacy Manager (zaawansowane)

Zamawianie i instalacja Certyfikatu Privacy Manager

Zanim będzie można skorzystać z funkcji programu Privacy Manager, musisz zamówić i zainstalować Certyfikat Privacy Manager (w programie Privacy Manager) za pomocą prawidłowego adresu e-mail. Adres e-mail musi być skonfigurowany jako konto w Microsoft Outlook na tym samym komputerze, na którym zamawiasz Certyfikat Privacy Manager.

Zamawianie Certyfikatu Privacy Manager

1. Otwórz Privacy Manager i kliknij **Certificates** (Certyfikaty).
2. Kliknij **Request a Privacy Manager certificate** (Zamów Certyfikat Privacy Manager).
3. Przeczytaj tekst powitalny, a następnie kliknij przycisk **Next** (Dalej).
4. Na stronie License Agreement (Umowa licencyjna), przeczytaj umowę.
5. Pamiętaj by zaznaczyć pole obok **Check here to accept the terms of this license agreement** (Zaznacz tutaj by zaakceptować warunki tej umowy licencyjnej), a następnie kliknij **Next** (Dalej).
6. Na stronie Your Certificate Details (Szczegółowe informacje certyfikatu), wpisz wymagane informacje i kliknij **Next** (Dalej).
7. Na stronie “Certificate Request Accepted” (Zaakceptowanie żądanie certyfikatu) kliknij **Finish** (Zakończ).
8. Kliknij przycisk **OK** by zamknąć certyfikat.

Otrzymasz wiadomość e-mail w Microsoft Outlook z dołączonym Certyfikatem Privacy Manager.

Uzyskiwanie wcześniej przypisanego Certyfikatu Privacy Manager dla przedsiębiorstw

1. W programie Outlook otwórz wiadomość zawierającą przypisany Certyfikat dla przedsiębiorstw.
2. Kliknij **Obtain** (Uzyskaj).
3. Otrzymasz wiadomość e-mail w Microsoft Outlook z dołączonym Certyfikatem Privacy Manager.
4. Informacje na temat instalacji certyfikatu znajdują się w Instalacja Certyfikatu Privacy Manager na stronie 50

Instalacja Certyfikatu Privacy Manager

1. Gdy otrzymasz wiadomość e-mail z załączonym Certyfikatem Privacy Manager, otwórz ją i kliknij przycisk **Setup** (Ustawienia) w prawym dolnym narożniku w wiadomości w Outlook 2007, lub lewym górnym narożniku w Outlook 2003.
2. Uwierzytelnij się za pomocą wybranej metody logowania.
3. Na stronie Certificate Installed (Zainstalowano certyfikat) kliknij przycisk **Next** (Dalej).
4. Na stronie Certificate Backup (Kopia zapasowa certyfikatu) wprowadź lokalizację i nazwę dla pliku kopii, lub kliknij **Browse** (Przeglądaj) by odnaleźć lokalizację.

   △ **OSTROŻNIE:** Pamiętaj by zapisać plik poza dyskiem twardym i przechowywać go w bezpiecznym miejscu. Plik ten powinien być wyłącznie do użytku właściciela i jest wymagany, jeśli będzie potrzeba przywrócić Certyfikat Privacy Manager i związane z nim klucze.

5. Wpisz i potwierdź hasło, a następnie kliknij przycisk **Next** (Dalej).
6. Uwierzytelnij się za pomocą wybranej metody logowania.
7. Jeśli wybierzesz rozpoczęcie procesu zapraszania Zaufanych kontaktów, postępuj według instrukcji na ekranie rozpoczynając od kroku 2 tego tematu: Dodawanie Zaufanych kontaktów za pomocą kontaktów Microsoft Outlook na stronie 54.

   – lub –

Jeśli klikniesz **Cancel** (Anuluj), skorzystaj z informacji zawartych w Dodawanie Zaufanego kontaktu na stronie 53 na temat dodawania Zaufanych kontaktów w późniejszym terminie.

Sprawdzanie informacji szczegółowych Certyfikatu Privacy Manager

1. Otwórz Privacy Manager i kliknij **Certificates** (Certyfikaty).
2. Kliknij Certyfikat Privacy Manager.
3. Kliknij **Certificate details** (Informacje szczegółowe Certyfikatu).
4. Po zakończeniu przeglądania informacji kliknij **OK**.

Odnawianie Certyfikatu Privacy Manager

Gdy kończy się ważność Certyfikatu Privacy Manager, pojawi się informacja o konieczności jego odnowienia:

1. Otwórz Privacy Manager i kliknij **Certificates** (Certyfikaty).
2. Kliknij **Renew certificate** (Odnów Certyfikat).
3. Postępuj według informacji na ekranie by zakupić nowy Certyfikat Privacy Manager.

UWAGA: Proces odnawiania certyfikatu Privacy Manager nie zastępuje starego Certyfikatu Privacy Manager. Musisz zakupić nowy Certyfikat Privacy Manager i zainstalować go za pomocą tej samej procedury opisanej w Zamawianie i instalacja Certyfikatu Privacy Manager na stronie 49.

Ustawianie domyślnego Certyfikatu Privacy Manager

Tylko Certyfikaty Privacy Manager widoczne są w programie Privacy Manager, nawet jeśli inne certyfikaty od innych wystawców są zainstalowane w komputerze.

Jeśli posiadasz kilka Certyfikatów Privacy Manager w komputerze, które zostały zainstalowane z poziomu Privacy Manager, możesz określić domyślny certyfikat:

1. Otwórz Privacy Manager i kliknij **Certificates** (Certyfikaty).
2. Kliknij Certyfikat Privacy Manager który chcesz użyć jako domyślny, a następnie kliknij **Set default** (Ustaw domyślny).
3. Kliknij **OK**.

UWAGA: Nie musisz korzystać z domyślnego Certyfikatu Privacy Manager. Z poziomu wielu funkcji Privacy Manager możesz wybrać dowolny Certyfikat Privacy Manager do użytku.

Usuwanie Certyfikatu Privacy Manager

Jeśli usuniesz Certyfikat Privacy Manager, nie możesz otworzyć plików lub przeglądać danych zaszyfrowanych za pomocą tego certyfikatu. Jeśli przypadkowo usuniesz Certyfikat Privacy Manager, możesz przywrócić go z pliku kopii zapasowej utworzonego w trakcie instalacji certyfikatu. Więcej informacji można znaleźć w części Przywracanie Certyfikatu Privacy Manager na stronie 52.

Usuwanie Certyfikatu Privacy Manager:

1. Otwórz Privacy Manager i kliknij **Certificates** (Certyfikaty).
2. Kliknij Certyfikat Privacy Manager który chcesz usunąć, a następnie kliknij **Advanced** (Zaawansowane).
3. Kliknij **Delete** (Usuń).
4. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij **Yes** (Tak).
5. Kliknij **Close** (Zamknij), a następnie **Apply** (Zastosuj).

Przywracanie Certyfikatu Privacy Manager

W trakcie instalacji certyfikatu Privacy Manager, wymagane jest utworzenie kopii zapasowej certyfikatu. Możesz także utworzyć kopię na stronie Migration (Migracja). Ta kopia zapasowa może być użyta w trakcie migracji do innego komputera lub odtwarzania certyfikatu na tym samym komputerze.

1. Otwórz Privacy Manager i kliknij **Migration** (Migracja).
2. Kliknij **Restore** (Przywróć).
3. Na stronie Migration File (Plik migracji) kliknij przycisk **Browse** (Przeglądaj), aby znaleźć plik .dppsm utworzony w trakcie wykonywania kopii, a następnie kliknij przycisk **Next** (Dalej).
4. Wprowadź hasło podane podczas tworzenia kopii, a następnie kliknij **Next** (Dalej).
5. Kliknij przycisk **Finish** (Zakończ).
6. Kliknij **OK**.

Więcej informacji można znaleźć w części Instalacja Certyfikatu Privacy Manager na stronie 50 lub Wykonywanie kopii zapasowej Certyfikatów Privacy Manager i Zaufanych kontaktów na stronie 68.

Unieważnianie Certyfikatu Privacy Manager

Jeśli przeczuwasz, że bezpieczeństwo Certyfikatu Privacy Manager zostało zagrożone, możesz unieważnić swój certyfikat:

UWAGA: Unieważniony Certyfikat Privacy Manager nie jest usuwany. Można go nadal wykorzystywać do przeglądania zaszyfrowanych plików.

1. Otwórz Privacy Manager i kliknij **Certificates** (Certyfikaty).
2. Kliknij **Advanced** (Zaawansowane).
3. Kliknij Certyfikat Privacy Manager który chcesz unieważnić, a następnie kliknij **Revoke** (Unieważnij).
4. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij **Yes** (Tak).
5. Uwierzytelnij się za pomocą wybranej metody logowania.
6. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Zarządzanie Zaufanymi kontaktami

Zaufane kontakty to użytkownicy, którzy wymienili się Certyfikatami Privacy Manager, umożliwiając tym samym bezpieczną komunikację ze sobą.

Trusted Contacts Manager umożliwia wykonanie następujących zadań:

- Przeglądanie szczegółowych informacji o Zaufanych kontaktach
- Usuwanie Zaufanych kontaktów
- Sprawdzanie stanu unieważnień dla Zaufanych kontaktów (zaawansowane)

Dodawanie Zaufanych kontaktów

Dodawanie Zaufanych kontaktów odbywa się w 3 krokach:

1. Wysyłasz zaproszenie e-mail do odbiorcy Zaufanego kontaktu.
2. Odbiorca Zaufanego kontaktu odpowiada na wiadomość.
3. Gdy otrzymasz odpowiedź e-mail od odbiorcy Zaufanego kontaktu, kliknij **Accept** (Zaakceptuj).

Możesz wysłać zaproszenia Zaufanych kontaktów do pojedynczych odbiorców lub wysłać zaproszenie do wszystkich kontaktów w książce adresowej Microsoft Outlook.

Skorzystaj z poniższych części by dodać Zaufane kontakty.

UWAGA: Aby odpowiedzieć na zaproszenie i zostać Zaufanym kontaktem, odbiorca Zaufanych kontaktów musi posiadać zainstalowany program Privacy Manager w komputerze, lub mieć zainstalowany inny program. Informacje na temat instalacji innego oprogramowania znajdują się na stronie internetowej DigitalPersona pod adresem http://DigitalPersona.com/PrivacyManager.

Dodawanie Zaufanego kontaktu

1. Otwórz program Privacy Manager, kliknij **Trusted Contacts Manager** (Menedżer zaufanych kontaktów), a następnie kliknij **Invite Contacts** (Zaproś kontakty).

   – lub –

   W programie Microsoft Outlook kliknij strzałkę w dół obok opcji **Send Securely** (Wyślij bezpiecznie), a następnie kliknij **Invite Contacts** (Zaproś kontakty).

2. Jeśli otworzy się okno Select Certificate (Wybierz certyfikat), kliknij Certyfikat Privacy Manager który chcesz użyć jako domyślny, a następnie kliknij **OK**.

3. Po wyświetleniu okna dialogowego Trusted Contact Invitation (Zaproszenie Zaufanego kontaktu) przeczytaj tekst i kliknij **OK**.

   Wiadomość e-mail zostanie automatycznie utworzona.

4. Wprowadź co najmniej jeden adres e-mail odbiorców, których chcesz dodać do Zaufanych kontaktów.

5. Edytuj tekst i wpisz swoje nazwisko (opcjonalnie).

6. Kliknij **Send** (Wyślij).

UWAGA: Jeśli nie posiadasz Certyfikatu Privacy Manager, komunikat poinformuje że musisz posiadać Certyfikat Privacy Manager w celu wysłania zaproszenia Zaufanego kontaktu. Kliknij **OK** by uruchomić kreatora zamawiania certyfikatu. Więcej informacji można znaleźć w części Zamawianie i instalacja Certyfikatu Privacy Manager na stronie 49.

7. Uwierzytelnij się za pomocą wybranej metody logowania.

UWAGA: Po otrzymaniu wiadomości e-mail przez odbiorcę Trusted Contact, musi on otworzyć wiadomość e-mail i kliknąć **Accept** (Akceptuj) w dolnym, prawym roku wiadomości, a następnie kliknąć **OK**, gdy pojawi się okno dialogowe z informacjami.

8. Po otrzymaniu odpowiedzi e-mail od odbiorcy, który zaakceptował status Trusted Contact, kliknij **Accept** (Akceptuj) w dolnym, prawym roku wiadomości.

   Otworzy się okno dialogowe potwierdzające poprawne dodanie do listy kontaktów Trusted Contacts.

9. Kliknij **OK**.

Dodawanie Zaufanych kontaktów za pomocą kontaktów Microsoft Outlook

1. Otwórz program Privacy Manager, kliknij **Trusted Contacts Manager** (Menedżer zaufanych kontaktów), a następnie kliknij **Invite Contacts** (Zaproś kontakty).

   – lub –

   W programie Microsoft Outlook kliknij strzałkę w dół obok opcji **Send Securely** (Wyślij bezpiecznie), a następnie kliknij **Invite All My Outlook Contacts** (Zaproś wszystkie kontakty Outlook).

2. Gdy otworzy się strona Trusted Contact Invitation (Zaproszenie Zaufanych kontaktów), wybierz adresy e-mail odbiorców, których chcesz dodać jako Zaufane kontakty, a następnie kliknij **Next** (Dalej).

3. Po otwarciu strony Sending Invitation (Wysyłanie zaproszenia) kliknij **Finish** (Zakończ).

   Wiadomość e-mail zawierająca wybrane adresy Microsoft Outlook jest tworzona automatycznie.

4. Edytuj tekst i wpisz swoje nazwisko (opcjonalnie).

5. Kliknij **Send** (Wyślij).

UWAGA: Jeśli nie posiadasz Certyfikatu Privacy Manager, komunikat poinformuje że musisz posiadać Certyfikat Privacy Manager w celu wysłania zaproszenia Zaufanego kontaktu. Kliknij **OK** by uruchomić kreatora zamawiania certyfikatu. Więcej informacji można znaleźć w części Zamawianie i instalacja Certyfikatu Privacy Manager na stronie 49.

6. Uwierzytelnij się za pomocą wybranej metody logowania.

UWAGA: Po otrzymaniu wiadomości e-mail przez odbiorcę Trusted Contact, musi on otworzyć wiadomość e-mail i kliknąć **Accept** (Akceptuj) w dolnym, prawym roku wiadomości, a następnie kliknąć **OK**, gdy pojawi się okno dialogowe z informacjami.

7. Po otrzymaniu odpowiedzi e-mail od odbiorcy, który zaakceptował status Trusted Contact, kliknij **Accept** (Akceptuj) w dolnym, prawym roku wiadomości.

Otworzy się okno dialogowe potwierdzające poprawne dodanie do listy kontaktów Trusted Contacts.

8. Kliknij **OK**.

Przeglądanie szczegółowych informacji o Zaufanych kontaktach

1. Otwórz Privacy Manager i kliknij **Trusted Contacts** (Zaufane kontakty).
2. Kliknij Zaufany kontakt.
3. Kliknij **Contact details** (Informacje szczegółowe o kontakcie).
4. Po zakończeniu przeglądania informacji kliknij **OK**.

Usuwanie Zaufanego kontaktu

1. Otwórz Privacy Manager i kliknij **Trusted Contacts** (Zaufane kontakty).
2. Kliknij Zaufany kontakt, który chcesz usunąć.
3. Kliknij **Delete contact** (Usuń kontakt).
4. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij **Yes** (Tak).

Sprawdzanie stanu unieważnień dla Zaufanego kontaktu

Sprawdzanie, czy Zaufany kontakt nie unieważnił swojego Certyfikatu Privacy Manager:

1. Otwórz Privacy Manager i kliknij **Trusted Contacts** (Zaufane kontakty).
2. Kliknij Zaufany kontakt.
3. Kliknij przycisk **Advanced** (Zaawansowane).

   Otworzy się okno Advanced Trusted Contact Management (Zaawansowane zarządzanie Zaufanymi kontaktami).
4. Kliknij **Check Revocation** (Sprawdź unieważnienie).
5. Kliknij **Close** (Zamknij).

Zadania ogólne

Program Privacy Manager można wykorzystywać z następującymi produktami Microsoft:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Używanie Privacy Manager w programie Microsoft Outlook

Gdy zainstalowany jest program Privacy Manager, przycisk Privacy (Prywatność) jest wyświetlany na pasku narzędzi programu Microsoft Outlook, a przycisk Send Securely (Wyślij bezpiecznie) jest wyświetlany na pasku narzędzi każdej wiadomości e-mail Microsoft Outlook. Gdy klikniesz strzałkę w dół obok **Privacy** (Prywatność) lub **Send Securely** (Wyślij bezpiecznie), możesz wybrać jedną z poniższych opcji:

- Sign and Send (Podpisz i wyślij; tylko przy przycisku Send Securely)—Opcja ta dodaje cyfrowy podpis do wiadomości e-mail i wysyła ją po uwierzytelnieniu za pomocą wybranej metody logowania.
- Seal for Trusted Contacts and Send (Zapieczętuj dla Zaufanych kontaktów i wyślij; tylko przy przycisku Send Securely)—Opcja ta dodaje cyfrowy podpis do wiadomości e-mail, szyfruje ją i wysyła po uwierzytelnieniu za pomocą wybranej metody logowania.
- Invite Contacts (Zaproś kontakty)—Opcja ta pozwala na wysłanie zaproszenia Zaufanych kontaktów. Więcej informacji można znaleźć w części Dodawanie Zaufanego kontaktu na stronie 53.
- Invite Outlook Contacts (Zaproś kontakty Outlook)—Opcja ta pozwala na wysłanie zaproszenia Zaufanych kontaktów do wszystkich kontaktów w książce adresowej Microsoft Outlook. Więcej informacji można znaleźć w części Dodawanie Zaufanych kontaktów za pomocą kontaktów Microsoft Outlook na stronie 54.
- Open the Privacy Manager software (Otwórz oprogramowanie Privacy Manager)—Opcje Certificates (Certyfikaty), Trusted Contacts (Zaufane kontakty) i Settings (Ustawienia) pozwala na otwarcie programu Privacy Manager w celu dodania, przeglądania, lub zmiany obecnych ustawień. Więcej informacji można znaleźć w części Konfigurowanie Privacy Manager w programie Microsoft Outlook na stronie 56.

Konfigurowanie Privacy Manager w programie Microsoft Outlook

1. Otwórz program Privacy Manager, kliknij **Settings** (Ustawienia), a następnie kliknij kartę **E-mail**.

   – lub –

   Na głównym pasku programu Microsoft Outlook kliknij strzałkę w dół obok opcji **Send Securely** (Wyślij bezpiecznie) (**Privacy** (Prywatność) w Outlook 2003), a następnie kliknij **Settings** (Ustawienia).

   – lub –

   Na pasku narzędzi wiadomości e-mail programu Microsoft Outlook kliknij strzałkę w dół obok opcji **Send Securely** (Wyślij bezpiecznie), a następnie kliknij **Settings** (Ustawienia).

2. Wybierz akcje, które chcesz wykonać w trakcie wysyłania bezpiecznej wiadomości e-mail i kliknij **OK**.

Podpisywanie i wysyłanie wiadomości e-mail

1. W programie Microsoft Outlook, kliknij **Nowa** lub **Odpowiedz**.
2. Wpisz wiadomość e-mail.
3. Kliknij strzałkę w dół obok opcji **Send Securely** (Wyślij bezpiecznie) (**Privacy** (Prywatność) w Outlook 2003), a następnie kliknij **Sign and Send** (Podpisz i wyślij).
4. Uwierzytelnij się za pomocą wybranej metody logowania.

Pieczętowanie i wysyłanie wiadomości e-mail

Zapieczętowane wiadomości e-mail, które są cyfrowo podpisane i zapieczętowane (zaszyfrowane) mogą być odczytywane tylko przez osoby wybrane z listy Zaufanych kontaktów.

Pieczętowanie i wysyłanie wiadomości e-mail do Zaufanego kontaktu:

1. W programie Microsoft Outlook, kliknij **Nowa** lub **Odpowiedz**.
2. Wpisz wiadomość e-mail.
3. Kliknij strzałkę w dół obok opcji **Send Securely** (Wyślij bezpiecznie) (**Privacy** (Prywatność) w Outlook 2003), a następnie kliknij **Seal for Trusted Contacts and Send** (Zapieczętuj dla Zaufanych kontaktów i wyślij).
4. Uwierzytelnij się za pomocą wybranej metody logowania.

Przeglądanie zapieczętowanej wiadomości e-mail

Gdy otworzysz zapieczętowaną wiadomość e-mail, etykieta zabezpieczeń jest wyświetlana w jej nagłówku. Etykieta zabezpieczeń zawiera następujące informacje:

- Jakie poświadczenia zostały użyte do weryfikacji tożsamości osoby podpisującej e-mail
- Produkt, który został użyty do weryfikacji poświadczeń osoby podpisującej e-mail

Używanie Privacy Manager z dokumentem Microsoft Office 2007

UWAGA: Program Privacy Manager może być użyty wyłącznie z dokumentami Microsoft Office 2007.

Po zainstalowaniu Certyfikatu Privacy Manager, przycisk Sign and Encrypt (Podpisz i zaszyfruj) jest wyświetlany z prawej strony paska narzędzi we wszystkich dokumentach Microsoft Word, Microsoft Excel i Microsoft PowerPoint. Gdy klikniesz strzałkę w dół obok **Sign and Encrypt** (Podpisz i zaszyfruj), możesz wybrać jedną z poniższych opcji:

- Sign Document (Podpisz dokument)—Ta opcja dodaje cyfrowy podpis do dokumentu.
- Add Signature Line Before Signing (Dodaj linię podpisu przed podpisaniem; tylko programy Microsoft Word i Microsoft Excel)—Domyślnie linia podpisu jest dodawana podczas podpisywania lub szyfrowania dokumentów Microsoft Word lub Microsoft Excel. Aby wyłączyć tę opcję, kliknij **Add Signature Line** (Dodaj linię podpisu), by usunąć zaznaczenie.
- Encrypt Document (Zaszyfruj dokument)—Ta opcja dodaje cyfrowy podpis i szyfruje dokument.
- Remove Encryption (Usuń szyfrowanie)—Ta opcja usuwa szyfrowanie z dokumentu.
- Open the Privacy Manager software (Otwórz oprogramowanie Privacy Manager)—Opcje Certificates (Certyfikaty), Trusted Contacts (Zaufane kontakty) i Settings (Ustawienia) pozwala na

otwarcie programu Privacy Manager w celu dodania, przeglądania, lub zmiany obecnych ustawień. Więcej informacji można znaleźć w części Zarządzanie certyfikatami programu Privacy Manager na stronie 49, Zarządzanie Zaufanymi kontaktami na stronie 53 lub Konfigurowanie Privacy Manager w programie Microsoft Office na stronie 58.

Konfigurowanie Privacy Manager w programie Microsoft Office

1. Otwórz program Privacy Manager, kliknij **Settings** (Ustawienia), a następnie kliknij kartę **Documents** (Dokumenty).

   – lub –

   Na pasku narzędzi dokumentu Microsoft Office kliknij strzałkę w dół obok opcji **Sign and Encrypt** (Podpisz i zaszyfruj), a następnie kliknij **Settings** (Ustawienia).

2. Wybierz akcje, które chcesz skonfigurować, a następnie kliknij **OK**.

Podpisywanie dokumentu Microsoft Office

1. W programie Microsoft Word, Microsoft Excel, lub Microsoft PowerPoint, utwórz i zapisz dokument.
2. Kliknij strzałkę w dół obok **Sign and Encrypt** (Podpisz i zaszyfruj), a następnie kliknij **Sign Document** (Podpisz dokument).
3. Uwierzytelnij się za pomocą wybranej metody logowania.
4. Po wyświetleniu okna z potwierdzeniem przeczytaj tekst i kliknij **OK**.

Jeżeli później zdecydujesz się na edycję dokumentu, wykonaj następujące kroki:

1. Kliknij przycisk **Office** w lewym górnym rogu ekranu.
2. Kliknij **Prepare** (Przygotuj), a następnie kliknij polecenie **Mark as Final** (Oznacz jako ostateczny).
3. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij **Yes** (Tak) i kontynuuj pracę.
4. Po zakończeniu edycji podpisz ponownie dokument.

Dodawanie linii podpisu podczas podpisywania dokumentu Microsoft Word lub Microsoft Excel

Program Privacy Manager pozwala na dodanie linii podpisu podczas podpisywania dokumentu Microsoft Word lub Microsoft Excel:

1. W programie Microsoft Word lub Microsoft Excel utwórz i zapisz dokument.
2. Kliknij menu **Początek**.
3. Kliknij strzałkę w dół obok **Sign and Encrypt** (Podpisz i zaszyfruj), a następnie kliknij **Add Signature Line Before Signing** (Dodaj linię podpisu przed podpisaniem).

   UWAGA: Znak wyboruj jest wyświetlony obok opcji Add Signature Line Before Signing (Dodaj linię podpisu przed podpisaniem) po jej wybraniu. Domyślnie opcja ta jest włączona.

4. Kliknij strzałkę w dół obok **Sign and Encrypt** (Podpisz i zaszyfruj), a następnie kliknij **Sign Document** (Podpisz dokument).
5. Uwierzytelnij się za pomocą wybranej metody logowania.

Dodawanie sugerowanych podpisujących do dokumentu Microsoft Word lub Microsoft Excel

Możesz dodać kilka linii podpisu do dokumentu poprzez zaproszenie sugerowanych podpisujących. Sugerowany podpisujący to użytkownik, który jest wyznaczony przez właściciela dokumentu Microsoft Word lub Microsoft Excel do dodania linii podpisu do dokumentu. Możesz być sugerowanym podpisującym, albo może to być inna osoba, która chce podpisać dokument. Przykładowo, jeśli przygotowujesz dokument, który wymaga podpisu wszystkich członków działu, możesz zawrzeć linie podpisów dla użytkowników na dole ostatniej strony dokumentu z instrukcją podpisania do danej daty.

Dodawanie sugerowanego podpisującego do dokumentu Microsoft Word lub Microsoft Excel:

1. W programie Microsoft Word lub Microsoft Excel utwórz i zapisz dokument.
2. Kliknij menu **Wstaw**.
3. W grupie **Tekst** na głównym pasku kliknij strzałkę w dół obok opcji **Signature Line** (Linia podpisu), a następnie kliknij **Privacy Manager Signature Provider** (Dostawca podpisu Privacy Manager).

   Zostanie otwarte okno Signature Setup (Konfiguracja podpisu).
4. W polu tesktowym pod **Suggested signer** (Sugerowany podpisujący) wprowadź nazwę sugerowanego podpisującego.
5. W polu tesktowym pod **Instructions to the signer** (Instrukcje dla podpisującego) wprowadź wiadomość dla sugerowanego podpisującego.

   UWAGA: Wiadomość ta pojawi się w miejscu tytułu i jest usuwana lub zamieniana na tytuł użytkownika po podpisaniu dokumentu.
6. Zaznacz pole **Show sign date in signature line** (Pokaż datę podpisu w linii podpisu) by pokazać datę.
7. Zaznacz pole **Show signer's title in signature line'** (Pokaż tytuł podpisującego w linii podpisu) by pokazać tytuł.

   UWAGA: Ponieważ właściciel dokumentu przypisuje sugerowanych podpisujących do swojego dokumentu, jeśli pola **Show sign date in signature line** (Pokaż datę podpisu w linii podpisu) i/lub **Show signer's title in signature line** (Pokaż tytuł podpisującego w linii podpisu) nie zostaną zaznaczone, sugerowany podpisujący nie będzie mógł wyświetlić daty i/lub tytułu w linii podpisu, nawet jeśli ustawienia dokumentu podpisującego są tak skonfigurowane.
8. Kliknij **OK**.

Dodawanie linii podpisu sugerowanego podpisującego

Gdy sugerowani podpisujący otworzą dokument, zobaczą swoje nazwiska w nawiasach, wskazujące że ich podpisy są wymagane.

Podpisywanie dokumentu:

1. Dwukrotnie kliknij odpowiednią linię podpisu.
2. Uwierzytelnij się za pomocą wybranej metody logowania.

   Linia podpisu zostanie pokazana zgodnie z ustawieniami określonymi przez właściciela dokumentu.

Szyfrowanie dokumentu Microsoft Office

Możesz zaszyfrować dokument Microsoft Office dla siebie i swoich Zaufanych kontaktów. Gdy zaszyfrujesz dokument i zamkniesz go, musisz wraz z Zaufanymi kontaktami wybranymi z listy uwierzytelnić się przed jego otwarciem.

Szyfrowanie dokumentu Microsoft Office:

1. W programie Microsoft Word, Microsoft Excel, lub Microsoft PowerPoint, utwórz i zapisz dokument.
2. Kliknij menu **Początek**.
3. Kliknij strzałkę w dół obok **Sign and Encrypt** (Podpisz i zaszyfruj), a następnie kliknij **Encrypt Document** (Zaszyfruj dokument).

   Zostanie otwarte okno Select Trusted Contacts (Wybierz Zaufane kontakty).
4. Kliknij nazwę Zaufanego kontaktu, który będzie mógł otworzyć dokument i sprawdzić jego zawartość.

   UWAGA: W celu wybrania wielu nazw Zaufanych kontaktów przytrzymaj wciśnięty klawisz ctrl i kliknij poszczególne nazwy.
5. Kliknij **OK**.

Jeżeli później zdecydujesz się na edycję dokumentu, wykonaj kroki opisane w Usuwanie szyfrowania z dokumentu Microsoft Office na stronie 60. Gdy szyfrowanie zostanie usunięte, możesz edytować dokument. Aby ponownie zaszyfrować dokument, postępuj zgodnie ze wskazówkami przedstawionymi w tej części.

Usuwanie szyfrowania z dokumentu Microsoft Office

Gdy usuniesz szyfrowanie z dokumentu Microsoft Office, nie będziesz wraz ze swoimi Zaufanymi kontaktami musieć uwierzytelniać się w celu otwarcia i sprawdzenia zawartości dokumentu.

Usuwanie szyfrowania z dokumentu Microsoft Office:

1. Otwórz zaszyfrowany dokument programu Microsoft Word, Microsoft Excel, lub Microsoft PowerPoint.
2. Uwierzytelnij się za pomocą wybranej metody logowania.
3. Kliknij menu **Początek**.
4. Kliknij strzałkę w dół obok **Sign and Encrypt** (Podpisz i zaszyfruj), a następnie kliknij **Remove Encryption** (Usuń szyfrowanie).

Wysyłanie zaszyfrowanego dokumentu Microsoft Office

Możesz załączyć zaszyfrowany dokument Microsoft Office do wiadomości e-mail bez podpisywania czy szyfrowania samej wiadomości. W tym celu utwórz i wyślij wiadomość e-mail z podpisanym lub zaszyfrowanym dokumentem, tak samo jak zwykłą wiadomość z załącznikiem.

Jednak dla optymalnego bezpieczeństwa zalecane jest szyfrowanie wiadomości e-mail podczas załączania podpisanego lub zaszyfrowanego dokumentu Microsoft Office.

Wykonaj następujące kroki by wysłać zapieczętowaną wiadomość e-mail z załączonym podpisanym i/lub zaszyfrowanym dokumentem Microsoft Office:

1. W programie Microsoft Outlook, kliknij **Nowa** lub **Odpowiedz**.
2. Wpisz wiadomość e-mail.
3. Załącz dokument Microsoft Office.
4. Dodatkowe instrukcje znajdują się w Pieczętowanie i wysyłanie wiadomości e-mail na stronie 57.

Przeglądanie podpisanego dokumentu Microsoft Office

UWAGA: Nie musisz posiadać Certyfikatu Privacy Manager w celu przeglądania podpisanego dokumentu Microsoft Office.

Podczas otwierania podpisanego dokumentu Microsoft Office, wyświetlana jest ikona podpisu cyfrowego na pasku stanu na dole okna dokumentu.

1. Kliknij ikonę **Digital Signatures** (Podpisy cyfrowe) by włączyć wyświetlanie okna dialogowe Signatures (Podpisy), które zawiera nazwy wszystkich użytkowników podpisujących dokument oraz datę każdego podpisu.
2. Aby zobaczyć dodatkowe informacje o każdym z podpisów, kliknij prawym przyciskiem nazwę w oknie Signatures (Podpisy) i wybierz Signature Details (Informacje o podpisie).

Przeglądanie zaszyfrowanego dokumentu Microsoft Office

Aby obejrzeć zaszyfrowany dokument Microsoft Office na innym komputerze, należy zainstalować na nim program Privacy Manager. Dodatkowo, musisz odtworzyć Certyfikat Privacy Manager użyty do zaszyfrowania tego pliku.

Zaufany kontakt chcący przejrzeć zaszyfrowany dokument Microsoft Office musi posiadać Certyfikat Privacy Manager, a program Privacy Manager musi być zainstalowany w jego komputerze. Dodatkowo, Zaufany kontakt musi zostać wybrany przez właściciela zaszyfrowanego dokumentu Microsoft Office.

Używanie Privacy Manager w programie Windows Live Messenger

Privacy Manager dodaje poniższe funkcje bezpiecznej komunikacji do programu Windows Live Messenger:

- **Secure chat** (Bezpieczna rozmowa)—Komunikaty są przesyłane za pomocą SSL/TLS (Secure Sockets Layer/Transport Layer Security) po protokole XML, tej samej technologii która zapewnia bezpieczeństwo transakcji e-commerce.
- **Recipient identification** (Identyfikacja odbiorcy)—Możesz zweryfikować obecność i tożsamość osoby przed wysłaniem wiadomości.
- **Signed messages** (Podpisane wiadomości)—Możesz elektronicznie podpisywać swoje wiadomości. Następnie, jeżeli wiadomość została zmodyfikowana, po otrzymaniu przez odbiorcę, zostanie oznaczona jako nieprawidłowa.
- **Hide/show feature** (Funkcja ukryj/pokaż)—Możesz ukryć dowolną z wiadomości lub wszystkie wiadomości w oknie Privacy Manager Chat. Możesz także wysłać wiadomość z ukrytą treścią. Do wyświetlenia wiadomości wymagane jest uwierzytelnienie.

- **Secure chat history** (Bezpieczna historia rozmowy)—Zapisy z sesji rozmowy są szyfrowane zanim zostaną zapisane i wymagają uwierzytelniania w celu ich zobaczenia.
- **Automatic locking/unlocking** (Automatyczne blokowanie/odblokowanie)—Możesz zablokować lub odblokować okno Privacy Manager Chat lub ustawić je, by blokowało się automatycznie po określonym czasie bezczynności.

Rozpoczynanie sesji rozmowy Privacy Manager

UWAGA: W celu użycia programu Privacy Manager Chat, obie strony muszą posiadać program Privacy Manager i zainstalowany Certyfikat Privacy Manager. Informacje na temat zamawiania i instalacji Certyfikatu Privacy Manager znajdują się w Zamawianie i instalacja Certyfikatu Privacy Manager na stronie 49.

1. Aby uruchomić Privacy Manager Chat w programie Windows Live Messenger, wykonaj jedną z poniższych procedur:

   a. Kliknij prawym przyciskiem dostępny kontakt w komunikatorze Live Messenger, a następnie wybierz **Rozpocznij aktywność**.

   b. Kliknij przycisk **Rozpocznij rozmowę**.

   – lub –

   a. Kliknij dwukrotnie dostępny kontakt w komunikatorze Live Messenger, a następnie kliknij **Zobacz listę aktywności**.

   b. Kliknij **Akcja**, a następnie kliknij **Rozpocznij rozmowę**.

   – lub –

   a. Prawym przyciskiem myszy kliknij ikonę **ProtectTools** w obszarze powiadomień, kliknij **Privacy Manager for HP ProtectTools**, a następnie wybierz **Rozpocznij rozmowę**.

   b. W Live Messenger, kliknij **Akcje: Rozpocznij aktywność**, a następnie wybierz **Privacy Manager Chat** (Rozmowa Privacy Manager).

   UWAGA: Każdy użytkownik musi być aktywny w Live Messenger, a użytkownicy muszą być wyświetlani w swoich oknach aktywności programu Live Messenger. Kliknij by wybrać aktywnego użytkownika.

   Privacy Manager wysyła zaproszenie do kontaktu by rozpocząć sesję Privacy Manager Chat. Gdy zostanie zaakceptowane przez zaproszony kontakt, otworzy się okno Privacy Manager Chat. Jeśli zaproszony kontakt nie posiada Privacy Manager, zostanie poproszony o jego pobranie.

2. Kliknij **Start**, aby rozpocząć bezpieczną rozmowę.

Konfiguracja Privacy Manager dla programu Windows Live Messenger

1. W Privacy Manager Chat, kliknij przycisk **Settings** (Ustawienia).

   – lub –

   W programie Privacy Manager, kliknij **Settings** (Ustawienia), a następnie kliknij kartę **Chat** (Rozmowa).

   – lub –

   W przeglądarce historii Live Messenger programu Privacy Manager, kliknij przycisk **Settings** (Ustawienia).

2. Aby określić czas, po którym Privacy Manager Chat zablokuje sesję, wybierz liczbę z listy **Lock session after _ minutes of activity** (Zablokuj sesję po _ minut działania).

3. Aby określić folder historii dla sesji rozmów, kliknij **Przeglądaj** aby wyszukać folder, a następnie kliknij **OK**.

4. W celu automatycznego zaszyfrowania i zapisania swoich sesji po ich zamknięciu, zaznacz pole wyboru **Automatically save secure chat history** (Automatycznie zapisuj historię bezpiecznej rozmowy).

5. Kliknij **OK**.

Rozmowa w oknie Privacy Manager Chat

Po uruchomieniu Privacy Manager Chat, okno Privacy Manager Chat otwiera się w programie Windows Live Messenger. Używanie Privacy Manager Chat jest podobne do podstawowego użycia Windows Live Messenger, poza tym, że dostępne są dodatkowe funkcje w oknie Privacy Manager Chat:

- **Save** (Zapisz)—Kliknij ten przycisk aby zapisać sesję rozmowy do foldera wskazanego w konfiguracji. Możesz także skonfigurować Privacy Manager Chat tak, aby automatycznie zapisać każdą sesją po jej zamknięciu.
- **Hide all**, **Show all** (Ukryj wszystko i Wyświetl wszystko)—Kliknij odpowiedni przycisk, aby rozwinąć lub zwinąć wiadomość wyświetlane w oknie Secure Communications (Bezpieczna komunikacja). Możesz także ukrywać i wyświetlać poszczególne wiadomości klikając na nagłówku wiadomości.
- **Are you there?** (Jesteś tam?)—Kliknij ten przycisk, aby zażądać autoryzacji od kontaktu.
- **Lock** (Zablokuj)—Kliknij ten przycisk, aby zamknąć okno Privacy Manager Chat i powrócić do okna wprowadzania wiadomości. W celu ponownego wyświetlenia okna Secure Communications (Bezpieczna komunikacja), kliknij **Resume the session** (Wznów sesję), a następnie dokonaj autoryzacji wybraną metodą.
- **Send** (Wyślij)—Kliknij ten przycisk, aby wysłać zaszyfrowaną wiadomość do rozmówcy.
- **Send signed** (Wyślij podpisane)—Zaznacz to pole, aby elektronicznie podpisać i zaszyfrować wiadomości. Następnie, jeżeli wiadomość została zmodyfikowana, po otrzymaniu przez odbiorcę, zostanie oznaczona jako nieprawidłowa. Przy każdym przesłaniu podpisanej wiadomości, konieczna jest autoryzacja.
- **Send hidden** (Wyślij ukryte)—Zaznacz to pole, aby zaszyfrować wiadomość wyświetlając przy tym tylko nagłówek. Odbiorca musi się autoryzować w celu odczytania wiadomości.

Przeglądanie historii czatu

Privacy Manager Chat: Przeglądarka historii Live Messenger wyświetla zaszyfrowane pliki sesji Privacy Manager Chat. Sesje można zapisać klikając **Save** (Zapisz) w oknie Privacy Manager Chat lub przez włączenie automatycznego zapisywania na karcie Chat (Rozmowa) w programie Privacy Manager. W przeglądarce, dla każdej sesji widoczna jest (zaszyfrowana) nazwa ekranu kontaktu, oraz data i czas rozpoczęcia oraz zakończenia sesji. Domyślnie sesje są wyświetlane dla wszystkich skonfigurowanych kont pocztowych. W celu wybrania tylko niektórych kont, można użyć menu **Display history for** (Wyświetl historię dla).

Przeglądarka umożliwia wykonanie następujących zadań:

- Pokazywanie wszystkich sesji na stronie 64
- Pokazywanie sesji dla wybranego konta na stronie 64
- Sprawdzanie identyfikatora sesji na stronie 65
- Przeglądanie sesji na stronie 65
- Wyszukiwanie określonego tekstu w sesjach na stronie 65
- Usuwanie sesji na stronie 65
- Dodawanie lub usuwanie kolumn na stronie 66
- Filtrowanie wyświetlanych sesji na stronie 66

Uruchamianie przeglądarki historii Live Messenger:

▲ W obszarze powiadomień po prawej stronie paska zadań kliknij prawym przyciskiem ikonę **HP ProtectTools** i kliknij **Privacy Manager: for HP ProtectTools**, a następnie kliknij **Live Messenger History Viewer**.

– lub –

▲ W sesji rozmowy, kliknij **History Viewer** (Przeglądarka historii) lub **History** (Historia).

Pokazywanie wszystkich sesji

Pokazywanie wszystkich sesji wyświetla odszyfrowaną Nazwę kontaktu ekranowego dla wybranej obecnie sesji i wszystkich sesji z tym samym kontem.

Pokazywanie wszystkich zapisanych sesji rozmowy:

1. W przeglądarce historii Live Messenger, kliknij prawym przyciskiem dowolną sesję i wybierz **Pokaż wszystkie sesje**.
2. Uwierzytelnij się za pomocą wybranej metody logowania.

   Nazwy ekranowe kontaktów są odszyfrowywane.
3. Kliknij dwukrotnie dowolną sesję by zobaczyć jej zawartość.

Pokazywanie sesji dla wybranego konta

Pokazywanie sesji wyświetla odszyfrowaną Nazwę ekranową kontaktu dla obecnie wybranej sesji.

Pokazywanie określonej sesji historii rozmów:

1. W przeglądarce historii Live Messenger, kliknij prawym przyciskiem dowolną sesję i wybierz **Pokaż sesję**.
2. Uwierzytelnij się za pomocą wybranej metody logowania.

   Nazwa ekranowa kontaktu jest odszyfrowywana.
3. Kliknij dwukrotnie pokazaną sesję by zobaczyć jej zawartość.

UWAGA: Dodatkowe sesje zaszyfrowane tym samym certyfikatem będą zawierały odblokowaną ikonę, wskazującą że można je zobaczyć po dwukrotnym kliknięciu w dowolną z tych sesji bez dodatkowego uwierzytelniania. Sesje zaszyfrowane innym certyfikatem będą zawierały zablokowaną ikonę, wskazującą że ich Nazwy ekranowe kontaktów czy zawartość będzie można zobaczyć dopiero po dalszym uwierzytelnieniu.

Sprawdzanie identyfikatora sesji

Sprawdzanie identyfikatora sesji:

- W przeglądarce historii Live Messenger, kliknij prawym przyciskiem dowolną pokazaną sesję i wybierz **Pokaż identyfikator sesji**.

Przeglądanie sesji

Przeglądanie sesji otwiera plik do obejrzenia. Jeśli sesja nie została wcześniej pokazana (wyświetlając odszyfrowaną Nazwę ekranową kontaktu), jest pokazywana w tym samym czasie.

Przeglądanie historii sesji Live Messenger:

1. W przeglądarce historii Live Messenger, kliknij prawym przyciskiem dowolną sesję i wybierz **Pokaż**.
2. Jeśli pojawi się komunikat, uwierzytelnij się za pomocą wybranej metody logowania.

   Zawartość sesji zostanie odszyfrowywana.

Wyszukiwanie określonego tekstu w sesjach

Możesz wyszukiwać tekst tylko w pokazanych (odszyfrowanych) sesjach wyświetlanych w oknie przeglądarki. Są to sesje, w których Nazwa ekranowa kontaktu jest wyświetlana zwykłym tekstem.

Wyszukiwanie tekstu w historii sesji rozmów:

1. W przeglądarce historii Live Messenger kliknij przycisk **Szukaj**.
2. Wprowadź tekst to wyszukania, skonfiguruj wybrane parametry i kliknij **OK**.

   Sesje zawierające ten tekst zostaną podświetlone w oknie przeglądarki.

Usuwanie sesji

1. Wybierz sesję historii rozmowy.
2. Kliknij **Usuń**.

Dodawanie lub usuwanie kolumn

Domyślnie w przeglądarce historii Live Messenger wyświetlane są 3 najczęściej używane kolumny. Możesz dodać dodatkowe kolumny do wyświetlenia lub usunąć kolumny z ekranu.

Dodawania kolumn do wyświetlenia:

1. Kliknij prawym przyciskiem dowolny nagłówek kolumny, a następnie wybierz **Dodaj/usuń kolumny**.
2. Wybierz nagłówek kolumny w lewym okienku, a następnie kliknij **Dodaj** aby dodać ją do prawego okienka.

Usuwanie kolumn z ekranu:

1. Kliknij prawym przyciskiem dowolny nagłówek kolumny, a następnie wybierz **Dodaj/usuń kolumny**.
2. Wybierz nagłówek kolumny w prawym okienku, a następnie kliknij **Usuń** aby przenieść ją do lewego okienka.

Filtrowanie wyświetlanych sesji

Lista sesji dla wszystkich kont wyświetlana jest w przeglądarce historii Live Messenger. Możesz także filtrować wyświetlane sesje wedle:

- Określonych kont. Informacje na ten temat można znaleźć w Wyświetlanie sesji dla wybranego konta na stronie 66.
- Zakresu dat. Informacje na ten temat można znaleźć w Wyświetlanie sesji dla zakresu dat na stronie 66.
- Różnych folderów. Informacje na ten temat można znaleźć w Wyświetlanie sesji zapisanych w innym folderze niż domyślny na stronie 66.

Wyświetlanie sesji dla wybranego konta

▲ W przeglądarce historii Live Messenger, wybierz konto z menu **Wyświetl historię dla**.

Wyświetlanie sesji dla zakresu dat

1. W przeglądarce historii Live Messenger kliknij ikonę **Filtr zaawansowany**.

   Zostanie otwarte okno Filtr zaawansowany.
2. Zaznacz pole wyboru **Wyświetlaj tylko sesje z określonego zakresu dat**.
3. W polach tesktowych **Od daty** i **Do daty**, wprowadź dzień, miesiąc i/lub rok, albo kliknij strzałkę obok kalendarza by wybrać daty.
4. Kliknij **OK**.

Wyświetlanie sesji zapisanych w innym folderze niż domyślny

1. W przeglądarce historii Live Messenger kliknij ikonę **Filtr zaawansowany**.
2. Zaznacz pole **Użyj alternatywnego folderu dla plików historii**.

3. Wprowadź położenie foldera lub kliknij **Przeglądaj** by wyszukać folder.
4. Kliknij **OK**.

Zadania zaawansowane

Migracja Certyfikatów programu Privacy Manager i Zaufanych kontaktów do innego komputera

Możesz bezpiecznie wyemigrować Certyfikaty Privacy Manager i Zaufane kontakty do innego komputera, lub wykonać kopię zapasową danych dla zabezpieczenia. W tym celu wykonaj kopię danych jako plik chroniony hasłem do miejsca w sieci lub na przenośne urządzenie pamięci masowej, a następnie przywróć plik na nowym komputerze.

Wykonywanie kopii zapasowej Certyfikatów Privacy Manager i Zaufanych kontaktów

W celu wykonania kopii zapasowej Certyfikatów Privacy Manager i Zaufanych kontaktów do pliku chronionego hasłem wykonaj następujące kroki:

1. Otwórz Privacy Manager i kliknij **Migration** (Migracja).
2. Kliknij **Backup** (Kopia zapasowa).
3. Na stronie Select Data (Wybierz dane) wybierz kategorie danych do umieszczenia w pliku migracji, a następnie kliknij przycisk **Next** (Dalej).
4. Na stronie Migration File (Plik migracji) wprowadź nazwę lub kliknij **Browse** (Przeglądaj), aby znaleźć lokalizację, a następnie kliknij **Next** (Dalej).
5. Wpisz i potwierdź hasło, a następnie kliknij przycisk **Next** (Dalej).

UWAGA: Przechowuj hasło w bezpiecznym miejscu, ponieważ jest ono niezbędne do odtworzenia pliku migracji.

6. Uwierzytelnij się za pomocą wybranej metody logowania.
7. Na stronie Migration File Saved (Zapisano plik migracji) kliknij **Finish** (Zakończ).

Odtwarzanie Certyfikatów Privacy Manager i Zaufanych kontaktów

W celu Odtworzenia Certyfikatów Privacy Manager i Zaufanych kontaktów na innym komputerze w ramach procesu migracji lub na tym samym komputerze, wykonaj następujące kroki:

1. Otwórz Privacy Manager i kliknij **Migration** (Migracja).
2. Kliknij **Restore** (Przywróć).
3. Na stronie Migration File (Plik migracji) kliknij **Browse** (Przeglądaj), aby odnaleźć plik, a następnie kliknij **Next** (Dalej).
4. Wprowadź hasło podane podczas tworzenia pliku kopii, a następnie kliknij **Next** (Dalej).
5. Na stronie Migration File (Plik migracji) kliknij **Finish** (Zakończ).

Centralne zarządzanie programem Privacy Manager

Instalacja programu Privacy Manager może być częścią zcentralizowanej instalacji, która została dostosowana przez administratora. Jedna lub kilka z poniższych funkcji może być włączona lub wyłączona:

- **Certificate use policy** (Zasady wykorzystywania certyfikatów)—Używanie certyfikatów Privacy Manager wystawionych przez Comodo może być ograniczone, możesz też mieć prawo do wykorzystania certyfikatów cyfrowych wystawionych przez innych wystawców.
- **Encryption policy** (Zasady szyfrowania)—Możliwości szyfrowania mogą być osobno włączone lub wyłączone dla programów Microsoft Office lub Outlook i Windows Live Messenger.

10 Program File Sanitizer for HP ProtectTools

File Sanitizer jest narzędziem, które pozwala na bezpieczne niszczenie danych cyfrowych (informacji osobistych lub plików, danych historycznych i pobieranych z Internetu lub innych komponentów danych) znajdujących się w komputerze i na okresowe oczyszczanie dysku twardego.

UWAGA: Ta wersja File Sanitizer obsługuje jedynie dysk systemowy.

Niszczenie

Niszczenie różni się od standardowego usuwania Windows® (znanego także jako proste usuwanie w File Sanitizer) tym, że gdy niszczysz zasoby za pomocą File Sanitizer, wykorzystywany jest algorytm zamazujący dane, co czyni praktycznie niemożliwym odzyskanie oryginalnego zasobu. Proste usuwanie Windows może pozostawić cały plik (lub zasób) nietknięty na dysku twardym, lub w stanie, w którym można wykorzystać metody kryminalistyczne do odzyskania pliku (czy zasobu).

Gdy wybierzesz profil niszczenia (High Security (Wysokie bezpieczeństwo), Medium Security (Średnie bezpieczeństwo), lub Low Security (Niskie bezpieczeństwo)), zdefiniowana lista zasobów i metoda usuwania są automatycznie wybierane w celu przeprowadzenia niszczenia. Możesz także utworzyć własny profil niszczenia, pozwalający na określenie liczby cykli niszczenia, zasobów które mają być objęte niszczeniem, potwierdzeń przed niszczeniem określonych zasobów oraz zasobów wyłączonych z niszczenia. Więcej informacji można znaleźć w części „Wybieranie lub tworzenie profilu niszczenia na stronie 74”.

Możesz ustawić automatyczny harmonogram niszczenia, a także ręcznie niszczyć zasoby gdy tylko zechcesz. Więcej informacji można znaleźć w części Ustawianie harmonogramu niszczenia na stronie 73, Ręczne niszczenie zasobu na stronie 78 lub Ręczne niszczenie wszystkich wybranych elementów na stronie 79.

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

Czyszczenie wolnej przestrzeni

Usuwanie zasobu w Windows nie usuwa całkowicie jego zawartości z dysku. System Windows usuwa jedynie odniesienie do tego zasobu. Treść zasobu pozostanie na dysku twardym do czasu, gdy inny zasób nadpisze ten sam obszar nowymi informacjami.

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

UWAGA: Czyszczenie wolnej przestrzeni jest przeznaczone dla zasobów usuniętych za pomocą Kosza Windows lub zasobów usuniętych ręcznie. Czyszczenie wolnej przestrzeni nie zapewnia dodatkowego bezpieczeństwa zniszczonych zasobów.

Możesz utworzyć automatyczny harmonogram czyszczenia wolnej przestrzeni, lub ręcznie uruchamiać czyszczenie wolnej przestrzeni za pomocą ikony **HP ProtectTools** w obszarze powiadomień po prawej stronie paska zadań. Więcej informacji można znaleźć w części Ustawianie harmonogramu czyszczenia wolnej przestrzeni na stronie 74, lub Ręczne aktywowanie czyszczenia wolnej przestrzeni na stronie 79.

Procedury konfiguracji

Otwieranie programu File Sanitizer

Otwieranie programu File Sanitizer:

1. Kliknij **Start**, **Wszystkie programy**, kliknij **HP**, a następnie **HP ProtectTools Security Manager**.
2. Kliknij **File Sanitizer**.

– lub –

- Kliknij dwukrotnie ikonę **File Sanitizer** znajdującą się na pulpicie.

– lub –

- Prawym przyciskiem myszy kliknij ikonę **HP ProtectTools** w obszarze powiadomień po prawej stronie paska zadań, a następnie wybierz polecenie **File Sanitizer** i kliknij **Open File Sanitizer** (Uruchom File Sanitizer).

Ustawianie harmonogramu niszczenia

UWAGA: Informacje na temat wybierania zdefiniowanych profili niszczenia lub tworzenia profilu niszczenia znajdują się w Wybieranie lub tworzenie profilu niszczenia na stronie 74.

UWAGA: Informacje na temat ręcznego niszczenia zasobów znajdują się w Ręczne niszczenie zasobu na stronie 78.

1. Uruchom File Sanitizer i kliknij **Shred** (Niszcz).
2. Wybierz opcję niszczenia:
   - **Windows shutdown** (Wyłączenie Windows)—Wybierz tę opcję by zniszczyć wszystkie wybrane zasoby w trakcie wyłączania Windows.

     UWAGA: Po wybraniu tej opcji, podczas wyłączania systemu pojawi się okno dialogowe proponujące niszczenie wybranych plików lub pominięcie tej procedury. Kliknij **Yes** (Tak), aby pominąć procedurę lub **No** (Nie), aby kontynuować niszczenie.

   - **Web browser open** (Otwarcie przeglądarki)—Wybierz tę opcję by zniszczyć wszystkie zasoby związane z Internetem, takie jak historia adresów URL, po otwarciu przeglądarki.
   - **Web browser quit** (Zamknięcie przeglądarki)—Wybierz tę opcję by zniszczyć wszystkie zasoby związane z Internetem, takie jak historia adresów URL, po zamknięciu przeglądarki.
   - **Key sequence** (Sekwencja klawiszy)—Wybierz tę opcję by rozpocząć niszczenie za pomocą sekwencji klawiszy.
   - **Scheduler** (Harmonogram)—Zaznacz pole **Activate Scheduler** (Uruchom harmonogram), wprowadź hasło Windows, a następnie wpisz dzień i czas przeznaczony na niszczenie wybranych zasobów.

   UWAGA: Plik .dll jest niszczony i usuwany z systemu tylko wtedy, gdy zostanie przeniesiony do kosza.
3. Kliknij **Apply** (Zastosuj), a następnie **OK**.

Ustawianie harmonogramu czyszczenia wolnej przestrzeni

UWAGA: Czyszczenie wolnej przestrzeni jest przeznaczone dla zasobów usuniętych za pomocą Kosza Windows lub zasobów usuniętych ręcznie. Czyszczenie wolnej przestrzeni nie zapewnia dodatkowego bezpieczeństwa zniszczonych zasobów.

Ustawianie harmonogramu czyszczenia wolnej przestrzeni:

1. Uruchom File Sanitizer i kliknij **Free Space Bleaching** (Czyszczenie wolnej przestrzeni).
2. Zaznacz pole **Activate Scheduler** (Uruchom harmonogram), wprowadź hasło Windows, a następnie wpisz dzień i czas przeznaczony na czyszczenie dysku.
3. Kliknij **Apply** (Zastosuj), a następnie **OK**.

UWAGA: Czyszczenie wolnej przestrzeni może trwać bardzo długo. Mimo że czyszczenie wolnej przestrzeni jest przeprowadzane w tle, komputer może działać wolniej z powodu większego wykorzystania procesora.

Wybieranie lub tworzenie profilu niszczenia

Możesz określić metodę usuwania i wybrać zasoby do zniszczenia przez wybór zdefiniowanego już profilu lub utworzenie własnego profilu.

Wybieranie zdefiniowanego profilu niszczenia

Gdy wybierzesz zdefiniowany profil niszczenia (High Security (Wysokie bezpieczeństwo), Medium Security (Średnie bezpieczeństwo), lub Low Security (Niskie bezpieczeństwo)), zdefiniowana lista zasobów i metoda usuwania jest wybierana automatycznie. Możesz kliknąć przycisk **View Details** (Pokaż szczegóły) by zobaczyć zdefiniowaną listę zasobów przeznaczonych do niszczenia.

Wybieranie zdefiniowanego profilu niszczenia:

1. Uruchom File Sanitizer i kliknij **Settings** (Ustawienia).
2. Kliknij zdefiniowany profil niszczenia.
3. Kliknij **View Details** (Pokaż szczegóły) by zobaczyć listę zasobów przeznaczonych do niszczenia.
4. W opcji **Shred the following** (Zniszcz następujące), zaznacz pole obok każdego zasobu, który chcesz potwierdzić przed zniszczeniem.
5. Kliknij **Apply** (Zastosuj), a następnie **OK**.

Dostosowanie profilu niszczenia

Gdy tworzysz profil niszczenia, określasz liczbę cykli niszczenia, zasoby które mają być objęte niszczeniem, potwierdzenia przed niszczeniem określonych zasobów oraz zasoby wyłączone z niszczenia:

1. Otwórz program File Sanitizer, kliknij **Settings** (Ustawienia), kliknij **Advanced Security Settings** (Zaawansowane ustawienia zabezpieczeń), a następnie kliknij **View Details** (Pokaż szczegóły).
2. Określ liczbę cykli niszczenia.

UWAGA: Wybrana liczba cykli niszczenia zostanie przeprowadzona dla każdego zasobu. Przykładowo, jeśli wybierzesz 3 cykle niszczenia, algorytm zamazujący dane zostanie wykonany 3 razy. Jeśli wybierzesz większą liczbę cykli niszczenia, niszczenie potrwa znacznie dłużej. Jednak im wyższa jest wybrana liczba cykli niszczenia, tym mniejsze jest prawdopodobieństwo odzyskania danych.

3. Wybierz zasób, który chcesz zniszczyć:
   a. W obszarze **Available shred options** (Dostępne opcje niszczenia), kliknij zasób, a następnie kliknij **Add** (Dodaj).
   b. W celu dodania własnego zasobu, kliknij **Add Custom Option** (Dodaj własną opcję) i przejdź do ścieżki lub wpisz nazwę pliku lub foldera. Kliknij **Open** (Otwórz), a następnie kliknij **OK**. W opcji **Available shred options** (Dostępne opcje niszczenia), kliknij własny zasób, a następnie kliknij **Add** (Dodaj).

UWAGA: Aby usunąć określony element z listy dostępnych opcji niszczenia, należy kliknąć ten element, a następnie kliknąć **Delete** (Usuń).

4. W opcji **Shred the following** (Zniszcz następujące), zaznacz pole obok każdego zasobu, który chcesz potwierdzić przed zniszczeniem

UWAGA: Aby usunąć określony zasób z listy do zniszczenia, kliknij ten zasób, a następnie kliknij **Remove** (Usuń).

5. W celu ochrony plików lub folderów przed automatycznym zniszczeniem w obszarze **Do not shred the following** (Nie niszcz następujących), kliknij **Add** (Dodaj), a następnie przejdź do pliku lub wpisz ścieżkę do pliku lub foldera. Kliknij **Open** (Otwórz), a następnie kliknij **OK**.

UWAGA: Aby usunąć określony zasób z listy wyjątków, kliknij ten zasób, a następnie kliknij **Delete** (Usuń).

6. Po zakończeniu konfigurowania profilu niszczenia kliknij **Apply** (Zastosuj), a następnie **OK**.

Dostosowanie profilu prostego usuwania

Profil prostego usuwania przeprowadza standardowe usuwanie zasobów bez niszczenia. Gdy dostosowujesz profil prostego usuwania, określasz zasoby które mają być objęte prostym usuwaniem, potwierdzenia przed usunięciem określonych zasobów oraz zasoby wyłączone z prostego usuwania.

UWAGA: Przy korzystaniu z opcji prostego usuwania, można okresowo przeprowadzać czyszczenie wolnych przestrzeni dla plików, które zostały usunięte ręcznie za pomocą kosza systemu Windows.

Dostosowanie profilu prostego usuwania:

1. Otwórz program File Sanitizer, kliknij **Settings** (Ustawienia), kliknij **Simple Delete Settings** (Ustawienia prostego usuwania), a następnie kliknij **View Details** (Pokaż szczegóły).
2. Wybierz zasób, który chcesz usunąć:
   a. W obszarze **Available delete options** (Dostępne opcje usuwania), kliknij zasób, a następnie kliknij **Add** (Dodaj).
   b. W celu dodania własnego zasobu, kliknij **Add Custom Option** (Dodaj własną opcję) i wpisz nazwę pliku lub foldera, a następnie kliknij **OK**. Kliknij własny zasób do dodania, a następnie kliknij **Add** (Dodaj).

UWAGA: Aby usunąć określony zasób z listy dostępnych usuwania, kliknij ten zasób, a następnie kliknij **Delete** (Usuń).

3. W opcji **Delete the following** (Usuń następujące), zaznacz pole obok każdego zasobu, który chcesz potwierdzić przed usunięciem.

UWAGA: Aby usunąć określony zasób z listy do usunięcia, kliknij ten zasób, a następnie kliknij **Remove** (Usuń).

4. W opcji **Do not delete the following** (Nie usuwaj następujących), kliknij **Add** aby zaznaczyć określony zasób, który chcesz wykluczyć z niszczenia.

UWAGA: Aby usunąć określony zasób z listy wyjątków, kliknij ten zasób, a następnie kliknij **Delete** (Usuń).

5. Po zakończeniu konfigurowania profilu prostego usuwania kliknij **Apply** (Zastosuj), a następnie **OK**.

Zadania ogólne

Możesz użyć program File Sanitizer do wykonywania następujących zadań:

- Use a key sequence to initiate shredding (użyj sekwencji klawiszy do rozpoczęcia niszczenia)—Funkcja ta pozwala na utworzenie sekwencji klawiszy (na przykład, ctrl+alt+s) do rozpoczęcia niszczenia. Informacje na ten temat można znaleźć w Używanie sekwencji klawiszy do rozpoczęcia niszczenia na stronie 77.
- Use the File Sanitizer icon to initiate shredding (Użyj ikony File Sanitizer do rozpoczęcia niszczenia)—Funkcja ta jest podobna do funkcji przeciągnij i upuść w Windows. Informacje na ten temat można znaleźć w Używanie ikony File Sanitizer na stronie 78.
- Manually shred a specific asset or all selected assets (Ręcznie zniszcz określony zasób lub wszystkie wybrane zasoby)—Funkcje te pozwalają na ręczne niszczenie elementów bez czekania na rozpoczęcie regularnego harmonogramu. Informacje na ten temat można znaleźć w Ręczne niszczenie zasobu na stronie 78 lub Ręczne niszczenie wszystkich wybranych elementów na stronie 79.
- Manually activate free space bleaching (Ręcznie aktywuj oczyszczanie wolnej przestrzeni)—Funkcja ta pozwala na ręczne aktywowanie oczyszczania wolnej przestrzeni. Informacje na ten temat można znaleźć w Ręczne aktywowanie czyszczenia wolnej przestrzeni na stronie 79.
- Abort a shred or free space bleaching operation (Ręcznie aktywuj oczyszczanie wolnej przestrzeni)—Funkcja ta pozwala na zatrzymanie operacji niszczenia lub oczyszczania wolnej przestrzeni. Informacje na ten temat można znaleźć w Przerywanie operacji niszczenia lub czyszczenia wolnej przestrzeni na stronie 79.
- View the log files (Zobacz pliki dziennika)—Funkcja ta pozwala na obejrzenie plików dziennika niszczenia i oczyszczania wolnej przestrzeni, zawierających błędy lub niepowodzenia z ostatniej operacji niszczenia lub oczyszczania wolnej przestrzeni. Informacje na ten temat można znaleźć w Przeglądanie plików dziennika na stronie 79.

UWAGA: Niszczenie lub oczyszczanie wolnej przestrzeni może trwać bardzo długo. Mimo że niszczenie i czyszczenie wolnej przestrzeni są przeprowadzane w tle, komputer może działać wolniej z powodu większego wykorzystania procesora.

Używanie sekwencji klawiszy do rozpoczęcia niszczenia

Wykonaj następujące kroki by utworzyć sekwencję klawiszy:

1. Uruchom File Sanitizer i kliknij **Shred** (Niszcz).
2. Zaznacz pole **Key sequence** (Sekwencja klawiszy).
3. Wprowadź literę w polu tesktowym.
4. Zaznacz pole **CTRL** lub **ALT**, a następnie zaznacz pole **SHIFT**.

   Przykładowo, by rozpocząć niszczenie za pomocą klawisza s i ctrl+shift, wprowadź znak `s` w polu i wybierz opcje **CTRL** i **SHIFT**.

UWAGA: Pamiętaj, by wybrać sekwencję klawiszy inną od pozostałych skonfigurowanych sekwencji.

Rozpoczynanie niszczenia za pomocą sekwencji klawiszy:

1. Podczas naciskania wybranego znaku, przytrzymuj naciśnięty klawisz shift oraz ctrl lub alt (lub inną wybraną kombinację).
2. Jeśli wyświetli się okno dialogowe z potwierdzeniem, kliknij **Yes** (Tak).

Używanie ikony File Sanitizer

△ **OSTROŻNIE:** Nie można odzyskać zniszczonych zasobów. Dokładnie przemyśl, które zasoby mają być wybrane do ręcznego niszczenia.

1. Przejdź do dokumentu lub foldera, który chcesz zniszczyć.
2. Przeciągnij zasób na ikonę **File Sanitizer** na pulpicie.
3. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij **Yes** (Tak).

Ręczne niszczenie zasobu

△ **OSTROŻNIE:** Nie można odzyskać zniszczonych zasobów. Dokładnie przemyśl, które zasoby mają być wybrane do ręcznego niszczenia.

1. Prawym przyciskiem myszy kliknij ikonę **HP ProtectTools** w obszarze powiadomień po prawej stronie paska zadań, a następnie wybierz polecenie **File Sanitizer** i kliknij **Shred One** (Zniszcz jeden).
2. Po wyświetleniu okna Browse (Przeglądaj), przejdź do zasobu który chcesz zniszczyć i kliknij **OK**.

UWAGA: Wybrany zasób może być pojedynczym plikiem lub folderem.

3. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij **Yes** (Tak).

– lub –

1. Kliknij dwukrotnie ikonę **File Sanitizer** znajdującą się na pulpicie i kliknij **Shred One** (Zniszcz jeden).
2. Po wyświetleniu okna Browse (Przeglądaj), przejdź do zasobu który chcesz zniszczyć i kliknij **OK**.
3. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij **Yes** (Tak).

– lub –

1. Uruchom File Sanitizer i kliknij **Shred** (Niszcz).
2. Kliknij przycisk **Browse** (Przeglądaj).
3. Po wyświetleniu okna Browse (Przeglądaj), przejdź do zasobu który chcesz zniszczyć i kliknij **OK**.
4. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij **Yes** (Tak).

Ręczne niszczenie wszystkich wybranych elementów

1. Prawym przyciskiem myszy kliknij ikonę **HP ProtectTools** w obszarze powiadomień po prawej stronie paska zadań, a następnie wybierz polecenie **File Sanitizer** i kliknij **Shred Now** (Zniszcz teraz).
2. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij **Yes** (Tak).

– lub –

1. Kliknij dwukrotnie ikonę **File Sanitizer** znajdującą się na pulpicie i kliknij **Shred Now** (Zniszcz teraz).
2. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij **Yes** (Tak).

– lub –

1. Uruchom File Sanitizer i kliknij **Shred** (Niszcz).
2. Kliknij przycisk **Shred now** (Niszcz teraz).
3. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij **Yes** (Tak).

Ręczne aktywowanie czyszczenia wolnej przestrzeni

1. Prawym przyciskiem myszy kliknij ikonę **HP ProtectTools** w obszarze powiadomień po prawej stronie paska zadań, a następnie wybierz polecenie **File Sanitizer** i kliknij **Bleach Now** (Czyść teraz).
2. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij **Yes** (Tak).

– lub –

1. Uruchom File Sanitizer i kliknij **Free Space Bleaching** (Czyszczenie wolnej przestrzeni).
2. Kliknij przycisk **Bleach Now** (Czyść teraz).
3. Po wyświetleniu okna dialogowego z potwierdzeniem kliknij **Yes** (Tak).

Przerywanie operacji niszczenia lub czyszczenia wolnej przestrzeni

Gdy wykonywana jest operacja niszczenia lub czyszczenia wolnej przestrzeni, wyświetlany jest komunikat nad ikoną HP ProtectTools Security Manager w obszarze powiadomienia. Komunikat zawiera informacje na temat procesu niszczenia lub czyszczenia wolnej przestrzeni (procent zakończenia) i daje opcję przerwania operacji.

Przerywanie operacji:

- Kliknij komunikat, a następnie kliknij przycisk **Stop** (Zatrzymaj), aby anulować operację.

Przeglądanie plików dziennika

Za każdym razem, gdy wykonywana jest operacja niszczenia lub czyszczenia wolnej przestrzeni, tworzone są pliki dziennika zawierające wszystkie błędy i niepowodzenia. Pliki dziennika są zawsze aktualizowane zgodnie z ostatnią operacją niszczenia lub czyszczenia wolnej przestrzeni.

UWAGA: Pliki, które zostały zniszczone lub wyczyszczone z powodzeniem nie pojawiają się w plikach dziennika.

Jeden plik dziennika tworzony jest dla operacji niszczenia, kolejny dla operacji czyszczenia wolnej przestrzeni. Oba pliki dziennika znajdują się na dysku twardym w folderze:

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

11 Program Device Access Manager for HP ProtectTools (tylko w wybranych modelach)

Administratorzy systemu operacyjnego Windows® używają programu Device Access Manager for HP ProtectTools do kontroli dostępu do urządzeń w systemie i ochrony przed nieautoryzowanym dostępem:

- Dla każdego użytkownika tworzony jest profil urządzeń określającym urządzenia, do których ma dostęp lub dostęp jest niemożliwy.
- Ponadto użytkownicy są zorganizowani w grupy, takie jak wstępnie zdefiniowana grupa Administratorów urządzeń; grupy mogą być także definiowane za pomocą opcji Zarządzanie komputerem dostępnej w sekcji Narzędzia administracyjne w Panelu sterowania.
- Udzielanie dostępu do urządzenia (lub odmowa tego dostępu) odbywa się na podstawie członkostwa w grupie.
- Można osobno zezwalać lub odmawiać dostępu do klas urządzeń, takich jak napędy CD-ROM i DVD, odczyt i zapis.

Użytkownicy z ograniczeniami mogą także uzyskać pozwolenie na odczytywanie i zmianę zasad dotyczących dostępu do urządzeń.

Procedury konfiguracji

Otwieranie programu Device Access Manager

Aby otworzyć program Device Access Manager, wykonaj następujące kroki:

1. Kliknij przycisk **Start**, **Wszystkie programy**, **HP**, a następnie **HP ProtectTools Administrative Console**.
2. W lewym okienku kliknij **Device Access Manager**.

Konfiguracja dostępu do urządzeń

Device Access Manager for HP ProtectTools zawiera trzy widoki:

- Widok Simple Configuration (Prosta konfiguracja) służy do dawania dostępu do klas urządzeń dla członków grupy Administratorzy urządzeń.
- Widok Device Class Configuration (Konfiguracja klasy urządzeń) służy do dawania dostępu do rodzajów urządzeń lub określonych urządzeń dla wybranych użytkowników lub grup.
- Widok User Access Settings (Ustawienia dostępu użytkowników) służy do określenia, którzy użytkownicy mogą przeglądać lub modyfikować informacje Simple Configuration (Prosta konfiguracja) i Device Class Configuration (Konfiguracja klasy urządzeń).

Grupa administratorów urządzeń

Po zainstalowaniu programu Device Access Manager tworzona jest grupa Device Administrators (Administratorzy urządzeń).

Administrator systemu może zastosować proste zasady kontroli dostępu do urządzeń poprzez uniemożliwienie dostępu do zestawu klas urządzeń, o ile użytkownik nie jest sklasyfikowany jako zaufany (w kwestii dostępu do urządzeń). Zalecanym sposobem na rozróżnienie pomiędzy "zaufanymi w kwestii urządzeń" użytkownikami, a użytkownikami "bez zaufania" jest uczynienie wszystkich "zaufanych w kwestii urządzeń" użytkowników członkami grupy Administratorów urządzeń. Dawanie członkom grupy Administratorów urządzeń dostępu do urządzeń za pomocą widoku Simple Configuration (Prosta konfiguracja) lub Device Class Configuration (Konfiguracja klas urządzeń) zapewni, że użytkownicy "zaufani w kwestii urządzeń" mają pełny dostęp do określonego zestawu klas urządzeń.

UWAGA: Dodanie użytkownika do grupy Administratorów urządzeń nie daje temu użytkownikowi automatycznie dostępu do urządzeń Jednak widok Simple Configuration (Prosta konfiguracja) może być użyty do zezwolenia dostępu do wybranego zestawu klas urządzeń dla "zaufanych w kwestii urządzeń" użytkowników.

Wykonaj następujące kroki by dodać użytkowników do grupy Administratorów urządzeń:

- W przypadku Windows 7, Vista, lub XP Professional, użyj standardowej przystawki “Użytkownicy i grupy lokalne” konsoli MMC.
- W przypadku wersji Home Windows 7, Vista®, lub XP, z poziomu konta z uprawnieniami wpisz poniższą komendę w oknie wiersza poleceń:

```
c:\> net localgroup “Device Administrators” nazwaużytkownika /ADD
```

Simple Configuration (Prosta konfiguracja)

Administratorzy i autoryzowani użytkownicy mogą użyć widoku Simple Configuration (Prosta konfiguracja) do zmiany praw dostępu do następujących klas urządzeń dla wszystkich użytkowników nie będących administratorami urządzeń:

UWAGA: W celu użycia tego widoku do odczytu informacji o dostępie do urządzeń, użytkownik lub grupa musi uzyskać dostęp "read" (odczyt) w widoku **User Access Settings** (Ustawienia dostępu użytkowników) W celu użycia tego widoku do zmiany informacji o dostępie do urządzeń, użytkownik lub grupa musi uzyskać dostęp "change" (zmiana) w widoku **User Access Settings** (Ustawienia dostępu użytkowników)

- Wszystkich nośników wymiennych (dyskietek, urządzeń flash USB itp.)
- Wszystkich napędów CD i DVD-ROM
- Wszystkich portów szeregowych i równoległych
- Wszystkich urządzeń Bluetooth®
- Wszystkich urządzeń podczerwieni
- Wszystkich modemów
- Wszystkich urządzeń PCMCIA
- Wszystkich urządzeń 1394

Wykonaj następujące kroki, aby zezwolić lub odmówić dostęp do klasy urządzeń wszystkim użytkownikom, którzy nie są administratorami urządzeń:

1. W lewym okienku **Konsoli administracyjnej HP ProtectTools**, kliknij **Device Access Manager**, a następnie pozycję **Simple Configuration** (Prosta konfiguracja).
2. By odmówić dostępu zaznacz w prawym okienku pole wyboru obok klasy urządzenia lub określonego urządzenia. Odznacz pole wyboru by zezwolić dostęp do tej klasy urządzenia lub określonego urządzenia.

   Jeśli pole wyboru jest wyszarzone, wartości wpływające na scenariusz dostępu zostały zmienione w widoku Device Class Configuration (Konfiguracja klasy urządzeń). Aby przywrócić te wartości do prostych ustawień, kliknij pole wyboru by je wyczyścić lub ustawić i kliknij **Yes** (Tak) by potwierdzić.
3. Kliknij ikonę **Save** (Zapisz).

   UWAGA: Jeśli usługa w tle nie działa, otworzy się okno dialogowe z pytaniem, czy chcesz ją uruchomić. Kliknij **Yes** (Tak).
4. Kliknij **OK**.

Uruchamianie usługi w tle

Zanim możliwe będzie zastosowanie profili urządzeń, program HP ProtectTools Security Manager wyświetla okno dialogowe z pytaniem, czy chcesz uruchomić usługę HP ProtectTools Device Locking/Auditing w tle. Kliknij **Yes** (Tak). Usługa w tle uruchomi się i będzie się od tego czasu uruchamiać przy starcie systemu.

UWAGA: Musisz zdefiniować profil urządzenia zanim zostanie wyświetlone pytanie o usługę w tle.

Administratorzy mogą także uruchomić lub zatrzymać tę usługę:

1. Kliknij przycisk **Start**, a następnie kliknij **Panel sterowania**.
2. Kliknij **Narzędzia administracyjne**, a następnie kliknij **Usługi**.
3. Poszukaj usługi **HP ProtectTools Device Locking/Auditing**.

Zatrzymanie usługi Device Locking/Auditing nie zatrzyma blokady urządzenia. Dwa elementy odpowiadają za blokadę urządzenia:

- Usługa Device Locking/Auditing
- Sterownik DAMDrv.sys

Uruchomienie usługi powoduje uruchomienie sterownika, ale zatrzymanie usługi nie zatrzymuje sterownika.

Aby sprawdzić czy usługa w tle działa, otwórz linię poleceń i wpisz sc query flcdlock.

Aby sprawdzić czy sterownik urządzenia działa, otwórz linię poleceń i wpisz sc query damdrv.

Device Class Configuration (Konfiguracja klasy urządzeń)

Administratorzy i autoryzowani użytkownicy mogą przeglądać i modyfikować listy użytkowników i grup, które mają pozwolenie lub jest im odmówiony dostęp do klas urządzeń lub określonych urządzeń.

UWAGA: W celu użycia tego widoku do odczytu informacji o dostępie do urządzeń, użytkownik lub grupa musi uzyskać dostęp "read" (odczyt) w widoku **User Access Settings** (Ustawienia dostępu użytkowników) W celu użycia tego widoku do zmiany informacji o dostępie do urządzeń, użytkownik lub grupa musi uzyskać dostęp "change" (zmiana) w widoku **User Access Settings** (Ustawienia dostępu użytkowników)

Widok Device Class Configuration (Konfiguracja klasy urządzeń) zawiera następujące części:

- **Device List** (Lista urządzeń)—Pokazuje wszystkie klasy urządzeń i urządzenia zainstalowane w systemie lub takie, które mogły być wcześniej zainstalowane w systemie.
  - Ochrona jest zazwyczaj stosowana dla klas urządzeń. Użytkownik lub wybrana grupa otrzyma dostęp do każdego urządzenia w danej klasie.
  - Ochrona może być także zastosowana do określonych urządzeń.
- **User List** (Lista użytkowników)—Pokazuje wszystkich użytkowników i grupy które które mają pozwolenie lub jest im odmówiony dostęp do wybranej klasy urządzeń lub określonego urządzenia.
  - Wpis User List (Lista użytkowników) można wykonać dla określonego użytkownika lub dla grupy, której użytkownik jest członkiem.
  - Jeśli wpis użytkownika lub grupy w User List (Lista użytkowników) jest niedostępny, ustawienie zostało odziedziczone z klasy urządzenia w Device List (Lista urządzeń) lub z foldera Class (Klasa).
  - Niektóre klasy urządzeń, takie jak DVD czy CD-ROM mogą podlegać dalszej kontroli przez zezwolenie lub odmowę osobno dla operacji odczytu i zapisu.

    Podobnie jak w przypadku innych urządzeń i klas, prawa dostępu do odczytu i zapisu mogą być dziedziczone. Przykładowo, prawo odczytu może być odziedziczone z wyższej klasy, ale prawo zapisu może być konkretnie odmówione dla użytkownika lub grupy.

UWAGA: Jeśli pole Read (Odczyt) nie jest zaznaczone, wówczas kontrola dostępu nie ma wpływu na prawo odczytu z urządzenia. Nie daje ani nie zabrania prawa odczytu z urządzenia.

Przykład 1—Jeśli użytkownikowi lub grupie odmówiono prawa zapisu w urządzeniu lub klasie urządzeń:

Ten sam użytkownik, ta sama grupa lub członek tej samej grupy może uzyskać prawo zapisu lub odczytu i zapisu tylko dla urządzenia poniżej tego urządzenia w hierarchii urządzeń.

Przykład 2—Jeśli użytkownikowi lub grupie dano prawo zapisu w urządzeniu lub klasie urządzeń:

Ten sam użytkownik, ta sama grupa lub członek tej samej grupy może mieć odmówione prawo zapisu lub odczytu i zapisu tylko dla tego samego urządzenia lub dla urządzenia poniżej tego urządzenia w hierarchii urządzeń.

Przykład 3—Jeśli użytkownikowi lub grupie dano prawo odczytu w urządzeniu lub klasie urządzeń:

Ten sam użytkownik, ta sama grupa lub członek tej samej grupy może mieć odmówione prawo odczytu lub odczytu i zapisu tylko dla tego samego urządzenia lub dla urządzenia poniżej tego urządzenia w hierarchii urządzeń.

Przykład 4—Jeśli użytkownikowi lub grupie odmówiono prawa odczytu w urządzeniu lub klasie urządzeń:

Ten sam użytkownik, ta sama grupa lub członek tej samej grupy może uzyskać prawo odczytu lub odczytu i zapisu tylko dla urządzenia poniżej tego urządzenia w hierarchii urządzeń.

Przykład 5—Jeśli użytkownikowi lub grupie dano prawo odczytu i zapisu w urządzeniu lub klasie urządzeń:

Ten sam użytkownik, ta sama grupa lub członek tej samej grupy może mieć odmówione prawo zapisu lub odczytu i zapisu tylko dla tego samego urządzenia lub dla urządzenia poniżej tego urządzenia w hierarchii urządzeń.

Przykład 6—Jeśli użytkownikowi lub grupie odmówiono prawa odczytu i zapisu w urządzeniu lub klasie urządzeń:

Ten sam użytkownik, ta sama grupa lub członek tej samej grupy może uzyskać prawo odczytu lub odczytu i zapisu tylko dla urządzenia poniżej tego urządzenia w hierarchii urządzeń.

Odmawianie dostępu użytkownikowi lub grupie

Wykonaj następujące kroki by uniemożliwić użytkownikowi lub grupie dostęp do urządzenia lub klasy urządzeń:

1. W lewym okienku **Konsoli administracyjnej HP ProtectTools**, kliknij **Device Access Manager**, a następnie pozycję **Device Class Configuration** (Konfiguracja klasy urządzeń).
2. Na liście urządzeń kliknij klasę urządzeń, którą chcesz skonfigurować.
   - Device class (Klasa urządzeń)
   - All devices (Wszystkie urządzenia)
   - Individual device (Pojedyncze urządzenie)

3. W obszarze **User/Groups** (Użytkownik/Grupy) dodaj użytkownika lub grupę, którym chcesz odmówić dostępu.
4. Kliknij **Deny** (Odmów) obok użytkownika lub grupy.
5. Kliknij ikonę **Save** (Zapisz).

UWAGA: Jeśli ustawienia odmowy i zezwolenia są nadane na tym samym poziomie urządzenia dla użytkownika, odmowa dostępu jest ważniejsza od zezwolenia.

Zezwalanie dostępu użytkownikowi lub grupie

Wykonaj następujące kroki by nadać uprawnienia użytkownikowi lub grupie na dostęp do urządzenia lub klasy urządzeń:

1. W lewym okienku **Konsoli administracyjnej HP ProtectTools**, kliknij **Device Access Manager**, a następnie pozycję **Device Class Configuration** (Konfiguracja klasy urządzeń).
2. Na liście urządzeń kliknij jedno z poniższych:
   - Device class (Klasa urządzeń)
   - All devices (Wszystkie urządzenia)
   - Individual device (Pojedyncze urządzenie)
3. Kliknij przycisk **Add** (Dodaj).

   Zostanie otwarte okno dialogowe **Select Users or Groups** (Wybierz użytkowników lub grupy).
4. Wybierz opcję **Advanced** (Zaawansowane), **Find Now** (Znajdź teraz), aby wyszukać użytkowników lub grupy do dodania.
5. Kliknij użytkownika lub grupę do dodania do listy dostępnych użytkowników i grup, a następnie kliknij **OK**.
6. Kliknij przycisk **OK** ponownie.
7. Kliknij **Allow** (Zezwalaj), aby udzielić dostępu temu użytkownikowi lub grupie.
8. Kliknij ikonę **Save** (Zapisz).

Odbieranie dostępu użytkownikowi lub grupie

Wykonaj następujące kroki by odebrać uprawnienia użytkownikowi lub grupie na dostęp do urządzenia lub klasy urządzeń:

1. W lewym okienku **Konsoli administracyjnej HP ProtectTools**, kliknij **Device Access Manager**, a następnie pozycję **Device Class Configuration** (Konfiguracja klasy urządzeń).
2. Na liście urządzeń kliknij klasę urządzeń, którą chcesz skonfigurować.
   - Device class (Klasa urządzeń)
   - All devices (Wszystkie urządzenia)
   - Individual device (Pojedyncze urządzenie)

3. W opcji **User/Groups** (Użytkownik/grupy), kliknij użytkownika lub grupę którą chcesz usunąć, a następnie kliknij przycisk **Remove** (Usuń).

4. Kliknij ikonę **Save** (Zapisz).

Umożliwienie dostępu do klasy urządzeń jednemu użytkownikowi lub grupie

Wykonaj następujące kroki w celu umożliwienia dostępu do klasy urządzeń jednemu użytkownikowi i odmówić go wszystkim pozostałym członkom danej grupy użytkowników:

1. W lewym okienku **Konsoli administracyjnej HP ProtectTools**, kliknij **Device Access Manager**, a następnie pozycję **Device Class Configuration** (Konfiguracja klasy urządzeń).

2. Na liście urządzeń kliknij klasę urządzeń, którą chcesz skonfigurować.

   - Device class (Klasa urządzeń)
   - All devices (Wszystkie urządzenia)
   - Individual device (Pojedyncze urządzenie)

3. W obszarze **User/Groups** (Użytkownik/Grupy) wybierz grupę, której chcesz odmówić dostępu i kliknij **Deny** (Odmów).

4. Nawiguj do folderu poniżej żądanej klasy, a następnie dodaj określonego użytkownika.

5. Kliknij **Allow** (Zezwalaj), aby udzielić dostępu danemu użytkownikowi.

6. Kliknij ikonę **Save** (Zapisz).

Umożliwienie dostępu do określonego urządzenia jednemu użytkownikowi lub grupie

Administratorzy mogą umożliwić dostęp do określonego urządzenia użytkownikowi i odmówić dostępu do wszystkich urządzeń należących do danej klasy wszystkim pozostałym członkom danej grupy użytkowników:

1. W lewym okienku **Konsoli administracyjnej HP ProtectTools**, kliknij **Device Access Manager**, a następnie pozycję **Device Class Configuration** (Konfiguracja klasy urządzeń).

2. Na liście urządzeń kliknij klasę urządzeń, którą chcesz skonfigurować, a następnie nawiguj do folderu poniżej.

3. Kliknij przycisk **Add** (Dodaj). Zostanie otwarte okno dialogowe **Select Users or Groups** (Wybierz użytkowników lub grupy).

4. Kliknij **Advanced** (Zaawansowane), a następnie kliknij **Find Now** (Znajdź teraz), aby wyszukać grupę użytkownika której ma być odmówiony dostęp do wszystkich urządzeń w klasie.

5. Kliknij grupę, a następnie kliknij **OK**.

6. Na liście urządzeń przejdź do określonego urządzenia w klasie urządzeń, do którego chcesz umożliwić dostęp użytkownikowi.

7. Kliknij przycisk **Add** (Dodaj). Zostanie otwarte okno dialogowe **Select Users or Groups** (Wybierz użytkowników lub grupy).

8. Wybierz opcję **Advanced** (Zaawansowane), **Find Now** (Znajdź teraz), aby wyszukać użytkowników lub grupy do dodania.

9. Kliknij użytkownika, któremu chcesz zapewnić dostęp, a następnie kliknij **OK**.

10. Kliknij **Allow** (Zezwalaj), aby udzielić dostępu danemu użytkownikowi.

11. Kliknij ikonę **Save** (Zapisz).

Resetowanie konfiguracji

△ **OSTROŻNIE:** Resetowanie konfiguracji odrzuca wszystkie dokonane zmiany konfiguracji i przywraca wszystkie ustawienia do wartości fabrycznych.

Wykonaj następujące kroki by zresetować ustawienia konfiguracji do wartości fabrycznych:

1. W lewym okienku **Konsoli administracyjnej HP ProtectTools**, kliknij **Device Access Manager**, a następnie pozycję **Device Class Configuration** (Konfiguracja klasy urządzeń).

2. Kliknij przycisk **Reset** (Resetuj).

3. Kliknij **Yes** (Tak) by potwierdzić.

4. Kliknij ikonę **Save** (Zapisz).

Zadania zaawansowane

Kontrola dostępu do ustawień konfiguracji

W widoku **User Access Settings** (Ustawienia dostępu użytkowników) administratorzy określają grupy lub użytkowników, którzy mogą korzystać ze stron Simple Configuration (Prosta konfiguracja) i Device Class Configuration (Konfiguracja klasy urządzeń).

UWAGA: Użytkownik lub grupa musi posiadać prawa "Full User Administrator rights" (Pełne uprawnienia administratora) w celu modyfikacji ustawień w widoku User Access Settings (Ustawienia dostępu użytkowników).

- Użytkownik lub grupa musi posiadać dostęp "View (Read-only) Configuration Settings" (Przeglądanie tylko do odczytu ustawień konfiguracji) w widoku User Access Settings (Ustawienia dostępu użytkowników) by móc przeglądać informacje Simple Configuration (Prosta konfiguracja) i Device Class Configuration (Konfiguracja klasy urządzeń).
- Użytkownik lub grupa musi posiadać dostęp "Change Configuration Settings" (Zmiana ustawień konfiguracji) w widoku User Access Settings (Ustawienia dostępu użytkowników) by móc zmieniać informacje Simple Configuration (Prosta konfiguracja) i Device Class Configuration (Konfiguracja klasy urządzeń).

UWAGA: Nawet członkowie grupy Administratorzy muszą uzyskać dostęp "read" (odczyt) by móc przeglądać widoki Simple Configuration (Prosta konfiguracja) i Device Class Configuration (Konfiguracja klasy urządzeń) oraz prawa "change" (zmiana) by móc zmieniać dane za pomocą widoków Simple Configuration (Prosta konfiguracja) i Device Class Configuration (Konfiguracja klasy urządzeń).

UWAGA: Po sprawdzeniu poziomów dostępu dla użytkowników i grup, jeśli dla użytkownika nie wybrano opcji Allow (Zezwól) ani Deny (Odmów) do danego poziomu dostępu, dostęp do tego poziomu zostanie odmówiony użytkownikowi.

Dawanie dostępu dla istniejącej grupy lub użytkownika

Wykonaj następujące kroki by dać zezwolenie istniejącej grupie lub użytkownikowi na przeglądanie lub zmianę ustawień konfiguracji:

1. W lewym okienku **Konsoli administracyjnej HP ProtectTools**, kliknij **Device Access Manager**, a następnie pozycję **User Access Settings** (Ustawienia dostępu użytkownika).
2. Kliknij grupę lub użytkownika którzy mają otrzymać prawo dostępu.
3. W opcji **Permissions** (Zezwolenia), kliknij **Allow** (Zezwól) przy każdym rodzaju zezwolenia nadanemu grupie lub użytkownikowi:

UWAGA: Otrzymane zezwolenia są narastające. Przykładowo, jeśli użytkownik otrzyma prawo “Change Configuration Settings” (Zmiana ustawień konfiguracji) automatycznie otrzymuje prawo “View (Read-only) Configuration Settings” (Przeglądanie tylko do odczytu ustawień konfiguracji). Użytkownik który otrzyma prawo “Full User Administrator Rights” (Pełne prawa administratora), otrzyma “Change Configuration Settings” (Zmiana ustawień konfiguracji) i “View (Read-only) Configuration Settings” (Przeglądanie tylko do odczytu ustawień konfiguracji).

- Full User Administrator Rights (Pełne prawa administratora)
- Change Configuration Settings (Zmiana ustawień konfiguracji)
- View (Read-only) Configuration Settings (Przeglądanie tylko do odczytu ustawień konfiguracji)

4. Kliknij ikonę **Save** (Zapisz).

Odmowa dostępu dla istniejącej grupy lub użytkownika

Wykonaj następujące kroki by odmówić prawa istniejącej grupie lub użytkownikowi do przeglądania lub zmiany ustawień konfiguracji:

1. W lewym okienku **Konsoli administracyjnej HP ProtectTools**, kliknij **Device Access Manager**, a następnie pozycję **User Access Settings** (Ustawienia dostępu użytkownika).
2. Kliknij grupę lub użytkownika którzy mają mieć odmówione prawo dostępu.
3. W opcji **Permissions** (Zezwolenia), kliknij **Deny** (Odmów) przy każdym rodzaju zezwolenia nadanemu grupie lub użytkownikowi:
   - Full User Administrator Rights (Pełne prawa administratora)
   - Change Configuration Settings (Zmiana ustawień konfiguracji)
   - View (Read-only) Configuration Settings (Przeglądanie tylko do odczytu ustawień konfiguracji)
4. Kliknij ikonę **Save** (Zapisz).

Dodawanie nowej grupy lub użytkownika

Wykonaj następujące kroki by dać zezwolenie nowej grupie lub użytkownikowi na przeglądanie lub zmianę ustawień konfiguracji:

1. W lewym okienku **Konsoli administracyjnej HP ProtectTools**, kliknij **Device Access Manager**, a następnie pozycję **User Access Settings** (Ustawienia dostępu użytkownika).
2. Kliknij przycisk **Add** (Dodaj). Zostanie otwarte okno dialogowe **Select Users or Groups** (Wybierz użytkowników lub grupy).
3. Wybierz opcję **Advanced** (Zaawansowane), **Find Now** (Znajdź teraz), aby wyszukać użytkowników lub grupy do dodania.
4. Kliknij grupę lub użytkownika, kliknij **OK**, a następnie ponownie kliknij **OK**.
5. Kliknij **Allow** (Zezwalaj), aby udzielić dostępu danemu użytkownikowi.
6. Kliknij ikonę **Save** (Zapisz).

Usuwanie dostępu dla grupy lub użytkownika

Wykonaj następujące kroki by odebrać prawo nowej grupie lub użytkownikowi do przeglądania lub zmiany ustawień konfiguracji:

1. W lewym okienku **Konsoli administracyjnej HP ProtectTools**, kliknij **Device Access Manager**, a następnie pozycję **User Access Settings** (Ustawienia dostępu użytkownika).
2. Kliknij grupę lub użytkownika, a następnie kliknij **Remove** (Usuń).
3. Kliknij ikonę **Save** (Zapisz).

Dokumentacja związana z tematem

Program Device Access Manager for HP ProtectTools jest zgodny z produktem dla przedsiębiorstw HP ProtectTools Enterprise Device Access Manager. Podczas pracy z produktem dla przedsiębiorstw, Device Access Manager for HP ProtectTools zezwala na dostęp tylko do odczytu do swoich funkcji.

Dodatkowe informacje na temat programu Device Access Manager for HP ProtectTools dostępne są na stronie internetowej pod adresem http://www.hp.com/hps/security/products.

12 LoJack Pro for HP ProtectTools

Linia produktów Absolute Software firmy Computrace umożliwia użytkownikom śledzenie komputerów HP i zwiększenie ochrony danych. Produkty Computrace LoJack zmniejszają liczbę utraconych urządzeń i pomagają w odnalezieniu skradzionych komputerów.

Jeżeli chcesz aktywować produkt Computrace, wykonaj poniższe kroki:

1. Kliknij **Start**, **Wszystkie programy**, a następnie **HP ProtectTools Security Manager**.
2. Kliknij **Theft Recovery** (Odzyskiwanie w przypadku kradzieży), a kliknij **Activate Now** (Aktywuj teraz).

   Uruchomi się domyślna przeglądarka i wyświetli się strona subskrypcji, na której można wybrać i zakupić jeden z trzech produktów Computrace dostępnych dla HP ProtectTools:

   - **Computrace Data Delete** (Kasowanie danych Computrace) — Obejmuje zdalne kasowanie danych, zamrożenie urządzenia i podstawowe śledzenie zasobów oraz raportowanie.
   - **Computrace LoJack Pro** — Obejmuje zdalne kasowanie danych, zamrożenie urządzenia i podstawowe śledzenie zasobów oraz raportowanie, a także zarządzane odzyskiwanie w przypadku kradzieży.
   - **Computrace LoJack Pro Premium** — Obejmuje zdalne kasowanie danych, zamrożenie urządzenia i podstawowe śledzenia zasobów oraz raportowanie, geolokację i geoograniczanie, a także zarządzane i odzyskiwanie w przypadku kradzieży.

Computrace Agent jest wbudowany w system BIOS notebooków HP dla biznesu, jednak w momencie dostarczenia Agent ten jest wyłączony. Po wykupieniu subskrypcji agent może być aktywowany. Wbudowany agent ma możliwość reinstalacji systemu operacyjnego i formatowania dysków twardych.

UWAGA: Dostępne są okresy subskrypcji od 1 do 5 lat. Dodatkowe informacje na ten temat znajdują się w umowie subskrypcyjnej firmy Absolute Software. Funkcja ta zależy od położenia geograficznego. Śledzenie GPS jest dostępne dla wybranych modeli z opcją WWAN.

13 Rozwiązywanie problemów

HP ProtectTools Security Manager

Krótki opis	Szczegóły	Rozwiązanie
Karty inteligentne i tokeny USB nie są dostępne w programie Security Manager jeśli zostały zainstalowane po instalacji Security Manager.	W celu wykorzystania kart inteligentnych i tokenów USB w programie Security Manager, obsługujące je oprogramowanie (sterowniki, dostawcy PKCS#11 itd.) musi być zainstalowane przed instalacją Security Manager. Jeśli oprogramowanie Security Manager jest już zainstalowane, wykonaj następujące kroki po instalacji oprogramowania obsługującego karty inteligentne i tokeny:	Zaloguj się do Password Manager. W HP ProtectTools Security Manager, kliknij **Password Manager**, kliknij **Credentials** (Poświadczenia), a następnie kliknij **Smart Card** (Karta inteligentna). Uruchom komputer ponownie jeśli pojawi się taka prośba.
Niektóre strony aplikacji sieci Web powodują błędy, uniemożliwiające użytkownikowi wykonywanie lub ukończenie zadań.	Niektóre aplikacje sieci Web przestają działać i zgłaszają wystąpienie błędów wywołane wyłączeniem funkcji jednokrotnego logowania. Na przykład w programie Internet Explorer jest wyświetlany znak **!** w żółtym trójkącie, co wskazuje na wystąpienie błędu.	Pojedyncze logowanie programu Security Manager nie obsługuje wszystkich interfejsów programistycznych stron internetowych. Wyłącz obsługę pojedynczego logowania dla wybranych stron przez wyłączenie obsługi funkcji Single Sign On (Pojedyncze logowanie). Skorzystaj z pełnej dokumentacji Single Sign On (Pojedyncze logowanie) dostępnej w pomocy oprogramowania Security Manager. Jeśli określonej funkcji jednokrotnego logowania dla danej aplikacji nie można wyłączyć, to skontaktuj się ze wsparciem technicznym firmy HP za pośrednictwem lokalnego punktu wsparcia HP i zamów wsparcie trzeciego poziomu.
Opcja **Browse for Virtual Token** (Wyszukaj token wirtualny) nie jest wyświetlana podczas logowania.	Użytkownik nie może zmienić położenia zarejestrowanego wirtualnego tokena w programie Password Manager, ponieważ opcja przeglądania została usunięta w celu zmniejszenia ryzyka zagrożenia.	Opcja wyszukiwania została usunięta, ponieważ umożliwia ona usuwanie i zmianę nazw plików oraz przejęcie kontroli nad systemem Windows przez osoby nieuprawnione.
Administratorzy domeny nie mogą zmienić hasła systemu Windows mimo uwierzytelnienia.	Dzieje się tak, gdy administrator loguje się do domeny i rejestruje tożsamość domeny w Password Manager za pomocą konta z prawami administratora w domenie i na lokalnym komputerze. Gdy administrator domeny próbuje zmienić hasło Windows w Password Manager, pojawia się błąd niepowodzenia logowania: **User account restriction** (Ograniczenie konta użytkownika).	Password Manager nie może zmienić hasła konta użytkownika domenowego za pomocą **Change Windows password** (Zmień hasło systemu Windows). Security Manager może zmieniać hasła tylko dla użytkowników lokalnych. Użytkownik domenowy może zmienić swoje hasło za pomocą opcji **Zmień hasło** w **Zabezpieczenia systemu Windows**, ale ponieważ użytkownik domenowy nie posiada fizycznego konta na kolejnym komputerze, Password Manager może zmienić tylko hasło użyte do zalogowania.

Krótki opis	Szczegóły	Rozwiązanie
Password Manager ma problemy ze zgodnością z hasłem Corel WordPerfect 12 o treści GINA.	Jeśli użytkownik loguje się do programu Password Manager, tworzy dokument w WordPerfect i zapisuje go chroniąc hasłem, Password Manager nie może wykryć lub rozpoznać, ręcznie ani automatycznie, hasła GINA.	Firma HP poszukuje obejścia tego problemu do zastosowania w przyszłych poprawkach produktu.
Password Manager nie rozpoznaje przycisku **Connect** (Połącz) na ekranie.	Jeśli poświadczenia jednokrotnego logowania dla podłączania pulpitu zdalnego (RDP) mają ustawiony przycisk **Połącz**, to po ponownym wywołaniu funkcji jednokrotnego logowania zawsze zamiast przycisku **Połącz** pojawia się przycisk **Zapisz jako**.	Firma HP poszukuje obejścia tego problemu do zastosowania w przyszłych poprawkach produktu.
Użytkownik nie może zalogować się do programu Password Manager po przełączeniu z trybu wstrzymania do hibernacji tylko w Windows XP Service Pack 1.	Po zezwoleniu systemowi na przełączenie do hibernacji i trybu uśpienia, Administrator lub użytkownik nie może zalogować się do programu Password Manager a ekran logowania Windows jest wyświetlany niezależnie od wybranego poświadczenia logowania (hasło, odcisk palca, lub karta Java Card).	Zaktualizuj Windows do Service Pack 2 poprzez Windows Update. Dodatkowe informacje na temat przyczyny tego problemu znajdują się w artykule bazy wiedzy Microsoft numer 813301 pod adresem http://www.microsoft.com. W celu zalogowania, użytkownik musi wybrać Password Manager i zalogować się. Po zalogowaniu do Password Manager, użytkownik jest proszony o zalogowanie do Windows (użytkownik może musieć wybrać opcję logowania Windows) w celu zakończenia procesu logowania. Jeśli użytkownik zaloguje się najpierw do Windows, wówczas musi się ręcznie zalogować do Password Manager.
Proces zabezpieczeń **Restore Identity** (Przywróć tożsamość) traci powiązanie z tokenem wirtualnym.	Gdy użytkownik odtwarza swoją tożsamość, Password Manager może utracić powiązania z lokalizacją wirtualnego tokenu na ekranie logowania. Mimo że wirtualny token jest zarejestrowany w Password Manager, użytkownik musi ponownie zarejestrować token w celu przywrócenia powiązania.	Jest to zgodne z obecnymi założeniami projektowymi. Podczas deinstalacji Password Manager bez zachowania tożsamości, część systemowa (serwer) tokena jest niszczona, tak więc token nie może już być użyty do logowania, nawet jeśli część kliencka tokena jest odtwarzana bez odtwarzania tożsamości. Firma HP bada długoterminowe możliwości rozwiązania tego problemu.

Device Access Manager for HP ProtectTools

Odmówiono dostępu do urządzeń użytkownikom w ramach Device Access Manager, ale urządzenia są wciąż dostępne.

- **Wyjaśnienie**—W programie Device Access Manager użyto opcji Simple Configuration (Prosta konfiguracja) i/lub Device Class Configuration (Konfiguracja klasy urządzeń) do odmowy dostępu użytkowników do urządzeń. Pomimo odmowy dostępu, użytkownicy wciąż mają dostęp do urządzeń.
- **Rozwiązanie:**
  - Sprawdź, czy usługa HP ProtectTools Device Locking jest uruchomiona.
  - Jako administrator, kliknij **Panel sterowania**, a następnie **System i konserwacja**. W oknie Narzędzia administracyjne kliknij **Usługi** i poszukaj usługi **HP ProtectTools Device Locking/ Auditing**. Sprawdź, czy usługa jest uruchomiona i czy typ uruchomienia to **Automatycznie**

Użytkownik niespodziewanie ma dostęp do urządzenia lub niespodziewanie odmówiono mu dostępu do urządzenia.

- **Wyjaśnienie**—Program Device Access Manager został użyty do odmowy dostępu dla użytkowników do niektórych urządzeń i zezwolenia na dostęp do innych urządzeń. Podczas używania systemu, mają oni dostęp do urządzeń, do których Device Access Manager miał odmówić dostępu i odmówiony dostęp do urządzeń, do których Device Access Manager powinien zezwolić na dostęp.
- **Rozwiązanie:**
  - Użyj funkcji Device Class Configuration (Konfiguracja klasy urządzeń) w programie Device Access Manager by sprawdzić ustawienia urządzeń dla użytkowników.
  - Kliknij **Security Manager**, kliknij **Device Access Manager**, a następnie kliknij **Device Class Configuration** (Konfiguracja klasy urządzeń). Rozwiń poziomy na drzewie Device Class (Klasa urządzeń) i przejrzyj ustawienia dotyczące tego użytkownika. Szukaj opcji “Deny” (Odmów) w zezwoleniach, która może być ustawiona dla tego użytkownika lub grupy Windows, której może on być członkiem, np. Użytkownicy, Administratorzy.

Zezwól czy odmów—które jest ważniejsze?

- **Wyjaśnienie**—W programie Device Class Configuration ustawiono następującą konfigurację:
  - Uprawnienie Pozwól zostało udzielone grupie użytkowników Windows (np. WBUDOWANE \Administratorzy), a uprawnienie Nie zezwalaj zostało udzielone innej grupie (np. WBUDOWANE\Users) na tym samym poziomie w hierarchii urządzeń (np. Napędy DVD/CD-ROM).
  - Jeśli użytkownik jest członkiem obu tych grup (np. Administratorzy), które jest ważniejsze?
- **Rozwiązanie:**
  - Użytkownik ma odmówiony dostęp do urządzenia. Opcja Deny (Odmów) jest ważniejsza od Allow (Zezwól).
  - Dostęp jest odmówiony z powodu sposobu, w jaki Windows rozpoznaje skuteczne pozwolenie dla urządzenia. Jedna z grup dostaje odmowę, druga otrzymuje zezwolenie, ale użytkownik jest członkiem obu grup. Użytkownik uzyskuje odmowę, ponieważ odmowa jest ważniejsza od nadania prawa dostępu.

- Jednym z obejść tego problemu jest odmowa dla grupy Użytkownicy na poziomie Napędy DVD/CD-ROM i pozwolenie dla grupy Administratorzy na poziomie poniżej Napędy DVD/CD-ROM.
- Inną metodą jest utworzenie specjalnej grupy Windows, jednej do udzielenia dostępu do DVD/CD, a drugiej do odmowy dostępu do DVD/CD. Odpowiedni użytkownicy zostaną wtedy dodani do odpowiedniej grupy.

Widok Simple Configuration (Prosta konfiguracja) został użyty do zdefiniowania zasad kontroli dostępu do urządzenia, ale administratorzy nie mają dostępu do urządzeń.

- **Wyjaśnienie**—Tryb Simple Configuration (Prosta konfiguracja) odmawia dostępu dla Użytkowników i Gości, ale zezwala go Administratorom urządzeń.
- **Rozwiązanie:** Dodaj Administratorów do grupy Administratorów urządzeń.

Różne

Dotyczy programu — krótki opis	Szczegóły	Rozwiązanie
Security Manager — jest wyświetlane ostrzeżenie: **The security application can not be installed until the HP Protect Tools Security Manager is installed** (Nie można zainstalować aplikacji zabezpieczeń przez zainstalowaniem programu HP Protect Tools Security Manager).	Wszystkie aplikacje zabezpieczające, takie jak Java Card Security (Zabezpieczenie kart Java Card) są rozszerzającymi wtyczkami dla interfejsu Security Manager. Security Manager musi być zainstalowany zanim będzie można załadować wtyczkę zabezpieczającą zatwierdzoną przez firmę HP.	Program Security Manager musi być zainstalowany przez instalacją dodatków plug-in zabezpieczeń.
HP ProtectTools Security Manager — Nieregularnie jest zgłaszany błąd podczas zamykania interfejsu programu Security Manager.	Nieregularnie (przeciętnie raz na 12 przypadków) po naciśnięciu przycisku zamykającego w prawym górnym narożniku okna programu Security Manager, zgłaszany jest błąd, spowodowany zamknięciem programu przed zakończeniem ładowania wszystkich dodatków plug-in.	Związane to jest z zależnościami czasowymi przy ładowaniu usług dodatków plug-in podczas zamykania i ponownego uruchamiania programu Security Manager. Ponieważ program PTHOST.exe jest powłoką łączącą inne aplikacje (dodatki plug-in), jest on zależny od możliwości zakończenia ładowania dodatków plug-in (usług) w określonym czasie. Zamknięcie powłoki przed zakończeniem ładowania dodatków plug-in jest podstawową przyczyną problemu. Poczekaj, aż zostanie wyświetlony komunikat o zakończeni ładowania usług (widoczny u góry okna programu Security Manager) i nazwy wszystkich dodatków plug-in pojawią się na liście w lewej kolumnie. Aby uniknąć błędu, poczekaj rozsądną chwilę, aby dodatki zostały załadowane.
HP ProtectTools — Nieograniczony dostęp do niekontrolowanych uprawnień administratora stanowi zagrożenie bezpieczeństwa.	Nieograniczony dostęp do komputera może być przyczyną wielu potencjalnych zagrożeń, między innymi następujących: • Usunięcie bezpiecznego dysku osobistego (PSD) • Złośliwa zmiana ustawień użytkownika • Wyłączenie zasad i funkcji zabezpieczeń	Zachęca się administratorów do przestrzegania "najlepszych wzorców" w ograniczaniu uprawnień użytkowników końcowych i ograniczaniu dostępu dla użytkowników. Nieautoryzowani użytkownicy nie powinni otrzymywać uprawnień administratora.

Słownik

Administrator **Zobacz** administrator Windows.

Administrator Windows Użytkownik mający pełne prawa do zmiany uprawnień i zarządzania innymi użytkownikami.

Aktywacja Zadanie, które musi zostać zakończone zanim jakakolwiek funkcja programu Drive Encryption będzie dostępna. Program Drive Encryption jest aktywowany za pomocą Kreatora instalacji HP ProtectTools. Tylko administrator może aktywować program Drive Encryption. Proces aktywacji składa się z aktywacji oprogramowania, szyfrowania dysku, tworzenia konta użytkownika, oraz tworzenia początkowej kopii klucza szyfrującego na przenośnym urządzeniu pamięci masowej.

Archiwum odzyskiwania awaryjnego Chroniony obszar przechowywania, który umożliwia ponowne szyfrowanie kluczy użytkownika podstawowego z jednego klucza właściciela platformy do innego.

ATM Automatic Technology Manager, umożliwia administratorom zdalne zarządzanie systemami na poziomie BIOS.

Automatyczne kasowanie Zaplanowane niszczenie ustawione przez użytkownika w programie File Sanitizer.

autoryzowany użytkownik Użytkownik, który otrzymał uprawnienia w widoku User Access Settings (Ustawienia dostępu użytkownika) do przeglądania lub zmiany ustawień konfiguracji w widokach Simple Configuration (Prosta konfiguracja) lub Device Class Configuration (Konfiguracja klasy urządzeń).

Bezpieczna komunikacja błyskawiczna Sesja komunikacyjna w trakcie której zaufane wiadomości są wysyłane przez zaufanego nadawcę do Zaufanych kontaktów.

Biometryczne Kategoria poświadczeń uwierzytelniania używających cechy fizycznej, takiej jak linie papilarne, w celu identyfikacji użytkownika.

Certyfikat cyfrowy Poświadczenia cyfrowe potwierdzające tożsamość osoby lub firmy poprzez łączenie tożsamości właściciela certyfikatu cyfrowego z parą kluczy elektronicznych używanych do podpisywania informacji cyfrowych.

Certyfikat menedżera prywatności Certyfikat cyfrowy wymagany do uwierzytelniania za każdym razem, gdy korzystasz z operacji kryptograficznych, takich jak podpisywanie i szyfrowanie wiadomości e-mail i dokumentów Microsoft Office.

Cykl kasowania Liczba powtórzeń wykonywania algorytmu niszczenia dla każdego zasobu. Im zostanie wybrana wyższa liczba cykli niszczenia, tym bezpieczniejszy komputer.

Czyszczenie wolnego miejsca Bezpieczne zapisywanie losowych danych na usuniętych zasobach w celu zamazania treści usuniętego zasobu.

Domena Grupa komputerów będąca częścią sieci i współdzieląca wspólną bazę danych katalogów. Domeny mają niepowtarzalne nazwy a każda posiada zestaw wspólnych zasad i procedur.

Dostawca usług kryptograficznych (CSP) Dostawca lub biblioteka algorytmów kryptograficznych, której można używać w dobrze zdefiniowanym interfejsie w celu wykonywania określonych funkcji kryptograficznych.

DriveLock Funkcja zabezpieczająca łącząca dysk twardy z użytkownikiem i wymagająca od użytkownika prawidłowego wpisania hasła DriveLock podczas uruchamiania komputera.

grupa Grupa użytkowników mających ten sam poziom dostępu lub odmowy dostępu do klasy urządzeń lub określonego urządzenia.

Hasło unieważnienia Hasło tworzone gdy użytkownik zażąda certyfikatu cyfrowego. Hasło jest wymagane gdy użytkownik chce unieważnić swój certyfikat cyfrowy. Dzięki temu tylko użytkownik może unieważnić certyfikat.

HP SpareKey Kopia zapasowa klucza szyfrującego napęd.

identyfikator Gadżet paska bocznego Windows służący do wzrokowej identyfikacji swojego pulpitu z nazwą użytkownika i wybranym obrazem. Kliknięcie Identyfikatora otwiera konsolę administracyjną HP ProtectTools.

Jednokrotne logowanie Funkcja przechowująca informacje uwierzytelniania i umożliwiająca korzystanie z programu Security Manager w celu uzyskiwania dostępu do aplikacji internetowych i aplikacji systemu Windows, które wymagają uwierzytelniania hasła.

Karta inteligentna Mały element sprzętowy podobny pod względem rozmiaru i kształtu do karty kredytowej, przechowujący informacje identyfikacyjne właściciela. Służy do uwierzytelniania właściciela komputera.

Karta Java Card Wyjmowalna karta wkładana do komputera. Zawiera informacje identyfikacyjne w celu logowania. Logowanie z kartą Java Card na ekranie logowania programu Drive Encryption wymaga włożenia karty Java Card i wpisania nazwy użytkownika i numeru PIN karty Java Card.

Kasuj Wykonanie algorytmu zamazującego dane znajdujące się w zasobie.

klasa urządzeń Wszystkie urządzenia danego typu, na przykład napędy.

Kolejność klawiszy Kombinacja określonych klawiszy, która po naciśnięciu rozpoczyna automatyczne niszczenie - na przykład ctrl+alt+s.

konsola Centralna lokalizacja, w której możesz uzyskać dostęp do funkcji i ustawień programu HP ProtectTools Administrative Console i nimi zarządzać.

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

Konto użytkownika systemu Windows Profil osoby upoważnionej do logowania się do sieci lub komputera.

kopia zapasowa Użyj funkcji kopii zapasowej by zapisać kopię ważnych informacji z oprogramowania do miejsca znajdującego się poza programem. Można ją potem użyć do odtworzenia informacji na tym samym komputerze, lub na innym.

Kryptografia Praktyka szyfrowania i odszyfrowywania danych, dzięki której dane mogą zdekodować tylko wybrane osoby.

Linia podpisu Miejsce przeznaczone na wizualne pokazanie podpisu cyfrowego. Gdy dokument jest podpisywany, wyświetlane są nazwa podpisującego i metoda weryfikacji. Data podpisania i tytuł podpisującego mogą być również umieszczone.

Lista zaufanych kontaktów Lista zawierająca Zaufane kontakty.

Live Messenger History Viewer Element Rozmowy programu Privacy Manager pozwalający na wyszukiwanie i przeglądanie sesji zaszyfrowanej historii rozmów.

login Obiekt wewnątrz programu Security Manager zawierający nazwę użytkownika i hasło (i prawdopodobnie inne wybrane informacje), których można użyć do logowania na stronach internetowych lub w innych programach.

metoda bezpiecznego logowania Metoda wykorzystywana do zalogowania do komputera.

Migracja Zadanie pozwalające na zarządzanie, odtwarzanie i przenoszenie Certyfikatów programu Privacy Manager i Zaufanych kontaktów.

Nazwa użytkownika i hasło Metoda w procesie uwierzytelniania, dzięki której użytkownik udowadnia, że jest uprawniony do wykonania określonego zadania.

Odbiorca zaufanego kontaktu Osoba, która otrzymuje zaproszenie do zostania Zaufanym kontaktem.

odciski palców Cyfrowy wyciąg z obrazu odcisku palca. Prawdziwy obraz odcisku palca nigdy nie jest przechowywany w programie Security Manager.

Odszyfrowywanie Procedura używana w kryptografii w celu konwersji zaszyfrowanych danych na zwykły tekst.

Okno logowania szyfrowania dysków Ekran logowania, który jest wyświetlany przed uruchomieniem systemu Windows. Użytkownik musi podać nazwę użytkownika Windows oraz hasło lub PIN karty Java Card. W większości przypadków podanie prawidłowych informacji na ekranie logowania Drive Encryption (Szyfrowanie dysku) pozwala od razu uzyskać bezpośredni dostęp do systemu Windows bez konieczności ponownego logowania na ekranie logowania Windows.

panel Centralna lokalizacja, w której możesz uzyskać dostęp do funkcji i ustawień programu HP ProtectTools Security Manager i nimi zarządzać.

Pieczęć dla zaufanych kontaktów Zadanie dodające podpis cyfrowy, szyfrujące wiadomość e-mail i wysyłające ją po uwierzytelnieniu za pomocą wybranej metody bezpiecznego logowania.

PIN Osobisty numer identyfikacyjny.

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

Podpis cyfrowy Dane wysyłane w pliku weryfikujące nadawcę materiału, oraz czy plik nie został zmodyfikowany po podpisaniu.

Pokaż Zadanie pozwalające użytkownikowi na odszyfrowanie jednej lub kilku sesji historii rozmów, wyświetlenie Nazwy ekranowej kontaktu w normalnym tekście i udostępnianie sesji do przeglądania.

Ponowne uruchomienie Proces ponownego uruchamiania komputera.

Profil kasowania Określona metoda usuwania i lista zasobów.

Proste kasowanie Usuwanie odnośnika Windows do zasobu. Treść zasobu pozostaje na dysku do czasu nadpisania danymi zamazującymi poprzez oczyszczanie wolnej powierzchni.

Przycisk Podpisz i zaszyfruj Przycisk programowy wyświetlany na pasku narzędzi aplikacji Microsoft Office. Kliknięcie przycisku pozwala na podpisanie, zaszyfrowanie lub usunięcie szyfrowania z dokumentu Microsoft Office.

Przycisk Wyślij zabezpieczone Przycisk programowy wyświetlany na pasku narzędzi wiadomości e-mail programu Microsoft Outlook. Kliknięcie przycisku pozwala na podpisanie i/lub zaszyfrowanie wiadomości e-mail programu Microsoft Outlook.

przywracanie Proces kopiujący informacje programu z uprzednio zapisanego pliku kopii zapasowej do tego programu.

PSD (Personal secure drive) Zapewnia chroniony obszar przechowywania poufnych danych.

Ręczne kasowanie Natychmiastowe niszczenie zasobu lub wybranych zasobów, pomijające harmonogram automatycznego niszczenia.

scena Zdjęcie zapisanego użytkownika wykorzystywane przy uwierzytelnianiu.

sesja historii rozmowy Zaszyfrowany plik zawierający zapis obu stron rozmowy w trakcie sesji rozmowy.

Sugerowany podpisujący Użytkownik, który jest wybrany przez właściciela dokumentu programów Microsoft Word i Microsoft Excel do dodania linii podpisu do dokumentu.

System szyfrowania plików (EFS) System szyfrujący wszystkie pliki i podfoldery w wybranym folderze.

Szyfrowanie Procedura, taka jak użycie algorytmu, stosowana w kryptografii w celu konwersji zwykłego tekstu na tekst zaszyfrowany, aby uniemożliwić nieupoważnionym odbiorcom odczytanie danych. Istnieje wiele typów szyfrowania danych i stanowią one podstawę zabezpieczeń sieciowych. Powszechnie stosowanymi typami są standard szyfrowania danych (DES) i szyfrowanie z użyciem klucza publicznego.

Szyfrowanie dysku Chroni dane poprzez zaszyfrowanie dysku, dzięki czemu informacje nie są czytelne dla osób nie posiadających właściwej autoryzacji.

Token Patrz Metoda bezpiecznego logowania.

Token USB Urządzenie zabezpieczające przechowujące informacje identyfikacyjne użytkownika. Podobnie jak karta Java Card czy czytnik biometryczny, używany jest do uwierzytelniania w komputerze jego właściciela.

Token wirtualny Funkcja zabezpieczająca, która działa w zasadzie tak samo jak karta Java Card lub czytnik kart. Token jest zapisywany na dysku twardym komputera lub w rejestrze Windows. Gdy zalogujesz się z wirtualnym tokenem, zostanie zadane pytanie o PIN użytkownika w celu zakończenia uwierzytelniania.

Tożsamość W programie HP ProtectTools Security Manager jest to grupa poświadczeń i ustawień obsługiwana tak jak konto lub profil określonego użytkownika.

Tryb natywny SATA Transfer danych pomiędzy komputerem a urządzeniami pamięci masowej, takimi jak dyski twarde i napędy optyczne.

TXT Trusted Execution Technology (Technologia zaufanego wykonywania).

Urząd certyfikacji Usługa wystawiająca certyfikaty wymagane do uruchomienia infrastruktury klucza publicznego.

usługa w tle Usługa w tle HP ProtectTools Device Locking/Auditing (Blokowanie/Inspekcja), która musi działać, by możliwe było stosowanie zasad kontroli dostępu do urządzeń. Można ją sprawdzić w aplikacji Usługi w opcji Narzędzia administracyjne w Panelu sterowania. Jeśli nie działa, program HP ProtectTools Security Manager spróbuje ją uruchomić po zastosowaniu zasad kontroli dostępu do urządzeń.

Uwierzytelnianie Proces weryfikacji, czy użytkownik jest autoryzowany do wykonania zadania, takiego jak uzyskanie dostępu do komputera, zmianę ustawień dla danego programu lub przeglądanie zabezpieczonych danych.

Uwierzytelnianie przy uruchamianiu komputera Funkcja zabezpieczeń wymagająca pewnej formy uwierzytelniania, takiej jak karta Java Card, układ elektroniczny zabezpieczeń lub hasło, przy włączaniu komputera.

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

Windows Logon Security (Zabezpieczenie logowania systemu Windows) Chroni konto(a) Windows poprzez wymaganie określonych poświadczeń w celu uzyskania dostępu.

Zaproszenie zaufanego kontaktu Wiadomość e-mail wysłana do osoby z pytaniem o zostanie Zaufanym kontaktem.

zasady kontroli dostępu do urządzeń Lista urządzeń, do których użytkownicy mogą uzyskać dostęp lub jest im on odmówiony.

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

Zaufana wiadomość Sesja komunikacyjna w trakcie której zaufane wiadomości są wysyłane przez zaufanego nadawcę do Zaufanych kontaktów.

Zaufany kontakt Osoba, która zaakceptowała zaproszenie Zaufanego kontaktu.

Zaufany nadawca Zaufany kontakt wysyłający podpisane i/lub zaszyfrowane wiadomości e-mail i dokumenty Microsoft Office.

Indeks

Z