HP ProtectTools
Gebruikershandleiding

© Copyright 2009 Hewlett-Packard Development Company, L.P.

Bluetooth is een handelsmerk van de desbetreffende houder en wordt door Hewlett-Packard Company onder licentie gebruikt. Java is een Amerikaans handelsmerk van Sun Microsystems, Inc. Microsoft en Windows zijn in de Verenigde Staten gedeponeerde handelsmerken van Microsoft Corporation.

De informatie in deze documentatie kan zonder kennisgeving worden gewijzigd. De enige garanties voor HP-producten en -diensten staan vermeld in de expliciete garantievoorwaarden bij de betreffende producten en diensten. Aan de informatie in deze handleiding kunnen geen aanvullende rechten worden ontleend. HP aanvaardt geen aansprakelijkheid voor technische fouten, drukfouten of weglatingen in deze publicatie.

Eerste editie, november 2009

Artikelnummer: 593308-331

Inhoudsopgave

1 Introductie tot beveiliging

De HP ProtectTools Security Manager software omvat beveiligingsvoorzieningen die bescherming bieden tegen ongeoorloofde toegang tot computers, netwerken en belangrijke gegevens. Het beheer van HP ProtectTools Security Manager vindt plaats via de voorziening Administrative Console.

Via de Administrative Console (beheerconsole) van HP ProtectTools kan de lokale beheerder de volgende taken uitvoeren:

- Beveiligingsvoorzieningen in- of uitschakelen
- Zijn/haar vingerafdrukken en die van andere gebruikers van deze computer registreren
- Een of meer scènes voor gezichtsverificatie registreren
- Smartcard instellen voor verificatiedoeleinden
- Opgeven welke referenties nodig zijn voor verificatie
- Gebruikers van de computer beheren
- Apparaatspecifieke parameters aanpassen
- Geïnstalleerde Security Manager applicaties configureren
- Extra Security Manager applicaties toevoegen

Via het dashboard van Security Manager kunnen algemene gebruikers de volgende taken uitvoeren:

- opties configureren die door een beheerder zijn verstrekt;
- beperkte bedieningsmogelijkheden van een aantal HP ProtectTools modules toestaan.

De softwaremodules die voor de computer beschikbaar zijn, kunnen per model verschillen.

De HP ProtectTools softwaremodules kunnen vooraf op de computer zijn geïnstalleerd of geladen, of zijn te downloaden op de website van HP. Ga naar http://www.hp.com voor meer informatie.

OPMERKING: in de instructies in deze handleiding wordt ervan uitgegaan dat u de voor uw computer beschikbare HP ProtectTools softwaremodules al op uw computer heeft geïnstalleerd.

Voorzieningen van HP ProtectTools

In de volgende tabel worden de voornaamste voorzieningen van de HP ProtectTools modules beschreven.

Module	Belangrijkste voorzieningen
HP ProtectTools Security Manager Administrative Console (voor beheerders)	• Veiligheidsniveaus en beveiligde aanmeldingsmethoden instellen en configureren met de Security Manager Setup Wizard. • Opties configureren die verborgen zijn voor basisgebruikers. • Configuraties en gebruikerstoegang voor Device Access Manager configureren. • HP ProtectTools gebruikers toevoegen en verwijderen en gebruikersstatussen weergeven met beheerprogramma's.
HP ProtectTools Security Manager (voor algemene gebruikers)	• Gebruikersnamen en wachtwoorden organiseren, instellen en wijzigen. • Gebruikersreferenties zoals Windows-wachtwoord en Smart Card configureren en wijzigen. • Shred (Versnipperen), Bleaching (Opschonen) en Settings (Instellingen) van File Sanitizer configureren en wijzigen. • Instellingen voor Device Access Manager weergeven. • Voorkeuren en opties voor Backup and Restore configureren.
Credential Manager for HP ProtectTools (Password Manager, wachtwoordbeheer)	• Uw namen en wachtwoorden opslaan, organiseren en beveiligen. • De aanmeldschermen voor websites en programma's instellen voor snelle en veilige toegang. • Gebruikersnamen en wachtwoorden voor websites opslaan door ze in te voeren in Password Manager. De volgende keer dat u een site bezoekt waarvoor u deze gegevens heeft ingevoerd, wordt de informatie automatisch ingevuld en verzonden door Password Manager. • Sterkere wachtwoorden maken voor een betere beveiliging van accounts. De informatie wordt automatisch ingevuld en verzonden door Password Manager.
Drive Encryption for HP ProtectTools (alleen bepaalde modellen)	• Zorgen voor codering van het volledige volume van vaste schijven. • Verificatie voorafgaand aan het opstarten vereisen om de gegevens te decoderen en toegankelijk te maken.
Privacy Manager for HP ProtectTools (alleen bepaalde modellen)	• Gebruikmaken van geavanceerde aanmeldingstechnieken om de bron, integriteit en veiligheid van communicatie te controleren van e-mail, Microsoft® Office-documenten of communicatie via expresberichten.

Module	Belangrijkste voorzieningen
File Sanitizer for HP ProtectTools	• Digitale middelen (gevoelige informatie waaronder applicatiebestanden, historische of internetgerelateerde inhoud of andere vertrouwelijke gegevens) op uw computer "versnipperen" en de vaste schijf periodiek opschonen.
Device Access Manager for HP ProtectTools (alleen bepaalde modellen)	• Systeembeheerders in staat stellen de toegang tot apparaten te regelen op basis van gebruikersprofielen. • Voorkomen dat onbevoegde gebruikers gegevens verwijderen middels externe opslagmedia en dat ze via externe media virussen in het systeem brengen. • Beheerders in staat stellen de toegang tot apparaten waarnaar kan worden geschreven te blokkeren voor specifieke gebruikers of groepen gebruikers.

Belangrijke beveiligingsdoelstellingen realiseren

De HP ProtectTools modules kunnen samenwerken om oplossingen te bieden voor verschillende beveiligingskwesties, waaronder de volgende belangrijke beveiligingsdoelstellingen:

- Bescherming bieden tegen gerichte diefstal
- Toegang tot gevoelige gegevens beperken
- Toegang door onbevoegden vanaf interne of externe locaties beperken
- Beleid met betrekking tot sterke wachtwoorden voorschrijven

Bescherming bieden tegen gerichte diefstal

Een voorbeeld van gerichte diefstal is wanneer op een controlepost op een vliegveld een computer wordt gestolen waarop vertrouwelijke gegevens en klantgegevens staan. De volgende voorzieningen bieden bescherming tegen gerichte diefstal:

- De verificatievoorziening vóór het opstarten, wanneer ingeschakeld, voorkomt toegang tot het besturingssysteem. Raadpleeg de volgende procedures:
  - Security Manager
  - Drive Encryption

Toegang tot gevoelige gegevens beperken

Stel dat een externe auditor op locatie werkt en toegang tot de computer heeft gekregen om gevoelige financiële gegevens te bekijken. In dat geval zult u niet willen dat de auditor de bestanden kan afdrukken of kan opslaan op een beschrijfbaar apparaat zoals een cd. Met de volgende voorziening wordt de toegang tot gegevens beperkt:

- Met Device Access Manager for HP ProtectTools kunnen IT-managers de toegang tot beschrijfbare apparaten beperken, zodat gevoelige gegevens niet kunnen worden afgedrukt of van de vaste schijf kunnen worden gekopieerd naar verwisselbare media.

Toegang door onbevoegden vanaf interne of externe locaties beperken

Toegang door onbevoegden tot een onbeveiligde bedrijfscomputer vormt een zeer reëel risico voor bronnen in bedrijfsnetwerken, zoals informatie van financiële diensten, een leidinggevende of een R&D-team, en voor privé-gegevens zoals patiëntendossiers of dossiers met persoonlijke financiële gegevens. De volgende voorzieningen helpen toegang door onbevoegden te voorkomen:

- De verificatievoorziening vóór het opstarten, wanneer ingeschakeld, voorkomt toegang tot het besturingssysteem. Raadpleeg de volgende procedures:
  - Password Manager
  - Drive Encryption
- Password Manager helpt voorkomen dat een niet-geautoriseerde gebruiker de beschikking krijgt over wachtwoorden of toegang krijgt tot met wachtwoord beveiligde applicaties.
- Met Device Access Manager for HP ProtectTools kunnen IT-managers de toegang tot beschrijfbare apparaten beperken, zodat gevoelige gegevens niet vanaf de vaste schijf kunnen worden gekopieerd.

- Met File Sanitizer kunt u gegevens veilig verwijderen door kritieke bestanden en mappen te versnipperen of door de vaste schijf op te schonen (gegevens overschrijven die zijn verwijderd maar nog kunnen worden hersteld).
- DriveLock zorgt ervoor dat gegevens ontoegankelijk zijn, zelfs als de vaste schijf wordt verwijderd en in een niet-beveiligd systeem wordt geïnstalleerd.

Beleid met betrekking tot sterke wachtwoorden voorschrijven

Als voor tientallen webapplicaties en -databases een beleid met sterke wachtwoorden moeten worden ingevoerd, biedt Security Manager een beveiligde opslagplaats voor wachtwoorden en het gemak van Single sign-on.

Extra beveiligingsonderdelen

Beveiligingsrollen toewijzen

Bij het beheren van computerbeveiliging (vooral voor grote organisaties) is het van belang om verantwoordelijkheden en rechten te verdelen over verschillende soorten beheerders en gebruikers.

OPMERKING: binnen een kleine organisatie of voor individueel gebruik kunnen deze rollen allemaal door dezelfde persoon worden vervuld.

Voor HP ProtectTools kunnen de beveiligingstaken en -rechten worden onderverdeeld in de volgende rollen:

- Beveiligingsmanager: definieert het beveiligingsniveau voor het bedrijf of netwerk en bepaalt de beveiligingsvoorzieningen die zullen worden ingezet, zoals Java™ Cards, biometrische lezers of USB-tokens.

  OPMERKING: veel van de voorzieningen in HP ProtectTools kunnen worden aangepast door degene die verantwoordelijk is voor de beveiliging, in samenwerking met HP. Ga naar de website van HP op http://www.hp.com voor meer informatie.

- Beheerder: past de door de beveiligingsmanager gedefinieerde beveiligingsvoorzieningen toe en beheert deze. De beheerder kan ook sommige voorzieningen in- en uitschakelen. Als de beveiligingsmanager bijvoorbeeld heeft besloten om Java Cards te gebruiken, kan de systeembeheerder de Java Card BIOS-beveiligingsmodus inschakelen.

- Gebruiker: gebruikt de beveiligingsvoorzieningen. Als de beveiligingsmanager en systeembeheerder bijvoorbeeld Java Cards hebben ingeschakeld voor het systeem, kan de gebruiker de pincode voor de Java Card instellen en de kaart gebruiken voor verificatiedoeleinden.

VOORZICHTIG: beheerders wordt aangeraden "optimale werkwijzen" toe te passen bij het beperken van de bevoegdheden van eindgebruikers en het beperken van gebruikerstoegang.

Aan onbevoegde gebruikers moeten geen beheerdersbevoegdheden worden toegekend.

Wachtwoorden van HP ProtectTools beheren

De meeste van de voorzieningen van HP ProtectTools Security Manager zijn beveiligd met wachtwoorden. In de volgende tabellen worden veelgebruikte wachtwoorden, de softwaremodule waarin het wachtwoord wordt ingesteld en de functie van het wachtwoord beschreven.

De wachtwoorden die zijn ingesteld en worden gebruikt door systeembeheerders, worden ook in deze tabel weergegeven. Alle andere wachtwoorden kunnen door regelmatige gebruikers of beheerders zijn ingesteld.

HP ProtectTools wachtwoord	Ingesteld in de volgende module	Functie
Windows-aanmeldwachtwoord	Windows® Configuratiescherm of HP ProtectTools Security Manager	Dit kan worden gebruikt voor handmatige aanmelding en voor verificatie om toegang te krijgen tot verschillende voorzieningen van Security Manager.

HP ProtectTools wachtwoord	Ingesteld in de volgende module	Functie
Backup and Recovery-wachtwoord van Security Manager	Security Manager, door individuele gebruiker	Beveiligt de toegang tot het Backup and Recovery-bestand van Security Manager.
Pincode Java™ Card	Java Card Security	Beschermt de inhoud van de Java Card en verifieert gebruikers ervan. Als de Java Card wordt gebruikt voor opstartverificatie, beschermt de pincode van de Java Card tevens het hulpprogramma Computer Setup (Computerinstellingen) en de inhoud van de computer. Verifieert gebruikers van Drive Encryption als het Java Card-token is geselecteerd.

Veilig wachtwoord maken

Volg bij het maken van wachtwoorden in de eerste plaats de vereisten van het programma. Neem echter over het algemeen de volgende richtlijnen in acht, om sterke wachtwoorden te creëren en de kans dat iemand uw wachtwoord te weten komt te verkleinen:

- Gebruik wachtwoorden van meer dan 6 tekens, bij voorkeur meer dan 8.
- Gebruik afwisselend hoofdletters en kleine letters in uw wachtwoord.
- Gebruik indien mogelijk afwisselend letters, cijfers, speciale tekens en leestekens.
- Vervang in een belangrijk woord letters door speciale tekens of getallen. Zo kunt u bijvoorbeeld het cijfer 1 gebruiken in plaats van de letter I of L.
- Combineer woorden uit twee of meer talen.
- Splits een woord of uitdrukking door middel van getallen of speciale tekens, bijvoorbeeld “Mary2-2Cat45”.
- Gebruik geen wachtwoord dat in een woordenboek voorkomt.
- Gebruik niet uw naam of andere persoonlijke informatie, zoals uw geboortedatum, namen van huisdieren of de meisjesnaam van uw moeder als wachtwoord, zelfs niet achterstevoren gespeld.
- Wijzig wachtwoorden regelmatig. U kunt wellicht eenvoudigweg enkele opvolgende tekens aanpassen.
- Als u uw wachtwoord opschrijft, zorg er dan voor dat u het niet op een zichtbare plaats in de buurt van de computer opbergt.
- Bewaar het wachtwoord niet in een bestand op de computer, zoals een e-mail.
- Deel accounts niet en vertel niemand uw wachtwoord.

Back-ups van HP ProtectTools referenties maken en terugzetten

Met de voorziening Backup and Restore van HP ProtectTools kunt u referentiegegevens en referentie-instellingen van HP ProtectTools selecteren en daarvan een back-up maken.

2 Aan de slag met de setup-wizard

De setup-wizard voor HP ProtectTools leidt u door de configuratie van de meest gebruikte voorzieningen van Security Manager. Via de HP ProtectTools Administrative Console zijn echter veel meer voorzieningen beschikbaar. Dezelfde instellingen die in de wizard aan bod komen, alsook extra beveiligingsvoorzieningen, kunnen worden geconfigureerd via de console, die kan worden geopend vanuit het menu Start van Windows®. Deze instellingen gelden voor de computer en alle gebruikers die de computer delen.

1. Een week nadat de computer is geïnstalleerd, wanneer u zich aanmeldt of wanneer een gebruiker met beheerdersrechten voor de eerste keer met een vinger over de vingerafdruklezer veegt, wordt de setup-wizard van Security Manager automatisch gestart om u door de algemene configuratiestappen voor het programma te leiden. Er wordt automatisch een zelfstudievideo gestart over het configureren van de computer.

   – of –

   Open HP ProtectTools Security Manager via het pictogram **Gadget** in de zijbalk van Windows of het taakbalkpictogram in het systeemvak aan de rechterkant van de taakbalk.

   

   De kleur van de bovenste balk op het pictogram Gadget geeft een van de volgende situaties aan:

   - Rood: HP ProtectTools is niet ingesteld, of er is een fouttoestand met een van de modules van ProtectTools.
   - Geel: raadpleeg de pagina Applications Status (Applicatiestatus) in Security Manager voor wijzigingen die moeten worden aangebracht in instellingen.
   - Blauw: HP ProtectTools is ingesteld en werkt naar behoren.

   OPMERKING: Het pictogram Gadget is niet beschikbaar in Windows XP.

   – of –

Klik achtereenvolgens op **Start**, **Alle programma's** en **HP ProtectTools Administrative Console**.

2. Lees de tekst op het welkomstscherm en klik op **Next** (Volgende).

OPMERKING: Op het welkomstscherm kunt u met een van de opties instellen dat de wizard niet opnieuw wordt weergegeven.

3. In de setup-wizard wordt u gevraagd uw identiteit te verifiëren.

   Typ uw Windows-wachtwoord of laat uw vingerafdrukken scannen door de vingerafdruklezer. Klik daarna op **Next** (Volgende).

   Als er geen vingerafdruklezer of smartcard beschikbaar is, wordt u verzocht om uw Windows-wachtwoord op te geven. In het vervolg moet u bij elke vereiste verificatie dit wachtwoord gebruiken.

   Als u nog geen Windows-wachtwoord heeft gemaakt, wordt u verzocht er een te maken. Een Windows-wachtwoord is vereist om uw Windows-account te beveiligen tegen toegang door onbevoegden en om de voorzieningen van HP ProtectTools Security Manager te kunnen gebruiken.

4. De setup-wizard leidt u door de stappen voor het instellen van de beveiligingsvoorzieningen die voor alle gebruikers van de computer gelden:

   - Met Aanmeldingsbeveiliging van Windows wordt uw Windows-accounts beveiligd doordat specifieke referenties nodig zijn om toegang te krijgen.
   - Drive Encryption beschermt uw gegevens door de vaste schijven te coderen, waardoor de gegevens onleesbaar zijn voor degenen die niet de juiste bevoegdheden hebben.
   - Pre-Boot Security beschermt de computer door onbevoegden de toegang te weigeren voordat wordt Windows opgestart.

     OPMERKING: Pre-Boot Security is niet beschikbaar als het BIOS van de computer daarvoor geen ondersteuning biedt.

   Als u een beveiligingsvoorziening wilt activeren, schakelt u het desbetreffende selectievakje in. Hoe meer voorzieningen u inschakelt, des te beter de computer is beveiligd.

5. Klik op de laatste pagina van de wizard op **Finish** (Voltooien).

   Het dashboard van Security Manager verschijnt.

OPMERKING: Als de wizard niet wordt voltooid, wordt de wizard nadien nog twee keer automatisch gestart. Daarna kunt u de wizard starten vanuit de waarschuwingsballon die in het systeemvak aan de rechterkant van de taakbalk wordt weergegeven (tenzij u deze heeft uitgeschakeld) totdat de configuratie is voltooid.

3 HP ProtectTools Security Manager Administrative Console

Het beheer van HP ProtectTools Security Manager vindt plaats via de Administrative Console (beheerconsole).

OPMERKING: Voor het beheer van HP ProtectTools zijn beheerdersbevoegdheden nodig.

De console biedt de volgende voorzieningen:

- Beveiligingsvoorzieningen in- of uitschakelen
- Gebruikers van de computer beheren
- Apparaatspecifieke parameters aanpassen
- Security Manager applicaties configureren
- Extra Security Manager applicaties toevoegen

▲ Als u de HP ProtectTools Security Manager applicaties wilt gebruiken, start u HP ProtectTools Security Manager vanuit het menu Start of klikt u met de rechtermuisknop op het pictogram Security Manager in het systeemvak, helemaal rechts op de taakbalk.

HP ProtectTools Administrative Console en de applicaties daarvan zijn beschikbaar voor alle gebruikers die de computer delen.

Administrative Console openen

Voor beheerderstaken, zoals het instellen van een systeembeleid of het configureren van software, opent u de console als volgt:

- Klik achtereenvolgens op **Start**, **Alle programma's**, **HP** en **HP ProtectTools Administrative Console**.

  – of –

  Klik in het linkerpaneel van het dashboard van Security Manager op **Administration** (Beheer).

Voor gebruikerstaken, zoals het registreren van vingerafdrukken of het gebruik van Security Manager, opent u de console als volgt:

- Klik achtereenvolgens op **Start**, **Alle programma's**, **HP** en **HP ProtectTools Security Manager**.

  – of –

  Dubbelklik op het pictogram **HP ProtectTools Security Manager** in het systeemvak helemaal rechts op de taakbalk.

Administrative Console gebruiken

De Administrative Console van Security Manager is de centrale locatie voor het beheer van HP ProtectTools Security Manager.

De beheerconsole bestaat uit de volgende onderdelen:

- **Tools** (Extra): hier ziet u de volgende configuratiecategorieën voor de beveiliging van de computer:
  - **Home** (Start): hier kunt u de beveiligingstaken selecteren die u wilt uitvoeren.
  - **System** (Systeem): hier kunt u de beveiligingsvoorzieningen en de verificatie voor gebruikers en apparaten configureren.
  - **Applications** (Applicaties): hier ziet u algemene instellingen voor HP ProtectTools Security Manager en voor de Security Manager applicaties.
  - **Data** (Gegevens): hier vindt u een uitvouwmenu met koppelingen naar Security Manager applicaties waarmee uw gegevens worden beveiligd.
- **Management Tools** (Beheerprogramma's): hier vindt u informatie over andere hulpmiddelen. In het paneel staan de volgende keuzemogelijkheden:
  - **HP ProtectTools Security Manager Setup Wizard** (Setup-wizard voor HP ProtectTools Security Manager): deze wizard leidt u door de configuratieprocedure voor HP ProtectTools Security Manager.
  - **Help**: hier wordt het helpbestand weergegeven, met daarin informatie over Security Manager en de vooraf geïnstalleerde applicaties van Security Manager. Hulpinformatie over applicaties die u kunt toevoegen, is te raadplegen vanuit de desbetreffende applicaties.
  - **About** (Info): hier vindt u informatie over HP ProtectTools Security Manager, zoals het versienummer en de auteursrechtgegevens.
- **Main area** (Hoofdgedeelte): hier worden applicatiespecifieke schermen weergegeven.

4 Systeem configureren

De groep System (Systeem) is toegankelijk via het paneel van het menu Tools (Extra) aan de linkerkant van het scherm van HP ProtectTools Administrative Console. Met de applicaties in deze groep kunt u de beleidsregels en instellingen voor de computer zelf en voor de gebruikers en apparaten van de computer beheren.

De volgende applicaties maken deel uit van de groep System (Systeem):

- **Security** (Beveiliging): hiermee beheert u voorzieningen, verificatie en instellingen voor de interactie tussen de computer en de gebruikers daarvan.
- **Users** (Gebruikers): hiermee kunt u gebruikers van de computer instellen, beheren en registreren.
- **Devices** (Apparaten): hiermee beheert u instellingen voor beveiligingsapparaten die in de computer zijn geïntegreerd of op de computer zijn aangesloten.

Verificatie instellen voor de computer

Binnen de applicatie Authentication (Verificatie) kunt u de beveiligingsvoorzieningen selecteren die u op de computer wilt implementeren, het toegangsbeleid voor de computer instellen en andere geavanceerde instellingen configureren. U kunt opgeven welke referenties nodig zijn voor de verificatie van gebruikersklassen wanneer gebruikers zich aanmelden bij Windows of wanneer zij zich tijdens een gebruikerssessie aanmelden bij websites en programma's.

U stelt als volgt verificatie op de computer in:

1. Klik in het menu van het paneel Security (Beveiliging) op **Authentication** (Verificatie).
2. Als u aanmeldingsverificatie wilt configureren, klikt u op het tabblad **Logon Policy** (Aanmeldbeleid), brengt u de gewenste wijzigingen aan en klikt u op **Apply** (Toepassen).
3. Als u sessieverificatie wilt configureren, klikt u op het tabblad **Session Policy** (Sessiebeleid), brengt u de gewenste wijzigingen aan en klikt u op **Apply** (Toepassen).

Aanmeldbeleid

U definieert als volgt beleidsregels voor de referenties die nodig zijn om een gebruiker te verifiëren wanneer deze zich aanmeldt bij Windows:

1. Klik in het menu Tools (Extra) op **Security** (Beveiliging) en klik vervolgens op **Authentication** (Verificatie).
2. Klik op het tabblad **Logon Policy** (Aanmeldbeleid) op een categorie gebruikers.
3. Geef de verificatiereferentie(s) op die voor de geselecteerde gebruikerscategorie nodig zijn. U moet minimaal één referentie opgeven.
4. Bepaal of één van de opgegeven referenties vereist is of álle opgegeven referenties vereist zijn om een gebruiker te verifiëren. U kunt ook voorkomen dat een gebruiker toegang tot de computer heeft.
5. Klik op **Apply** (Toepassen).

Sessiebeleid

U definieert als volgt beleidsregels voor de referenties die nodig zijn om tijdens een Windows-sessie toegang te krijgen tot HP ProtectTools applicaties:

1. Klik in het menu Tools (Extra) op **Security** (Beveiliging) en klik vervolgens op **Authentication** (Verificatie).
2. Klik op het tabblad **Session Policy** (Sessiebeleid) op een categorie gebruikers.
3. Geef de verificatiereferentie(s) op die voor de geselecteerde gebruikerscategorie nodig zijn.
4. Kies of EEN van de opgegeven referenties is vereist, of dat ALLE opgegeven referenties zijn vereist om een gebruiker te verifiëren. U kunt ook opgeven dat geen verificatie vereist is om toegang tot de HP ProtectTools software te krijgen.
5. Klik op **Apply** (Toepassen).

Instellingen

U kunt een of meer van de volgende beveiligingsinstellingen toestaan:

- **Allow One Step logon** (Aanmelding in één stap toestaan): Als deze optie is geselecteerd, kunnen gebruikers van deze computer de Windows-aanmelding overslaan als op BIOS-niveau of op gecodeerdeschijfniveau verificatie heeft plaatsgevonden.
- **Allow HP SpareKey authentication for Windows logon** (HP SpareKey verificatie toestaan voor Windows-aanmelding): Als deze optie is geselecteerd, kunnen gebruikers van deze computer gebruikmaken van de HP SpareKey functie om zich bij Windows aan te melden, ook als in Security Manager een ander verificatiebeleid is opgegeven.

U bewerkt de instellingen als volgt:

1. Klik om een specifieke instelling in of uit te schakelen.
2. Klik op **Apply** (Toepassen) om de aangebrachte wijzigingen op te slaan.

Gebruikers beheren

Binnen de applicatie Users (Gebruikers) kunt u de gebruikers van HP ProtectTools op deze computer bewaken en beheren.

Alle gebruikers van HP ProtectTools worden vermeld en geverifieerd aan de hand van de beleidsregels die via Security Manager zijn ingesteld. Bovendien wordt gecontroleerd of zij de juiste referenties hebben geregistreerd waarmee zij aan die beleidsregels kunnen voldoen.

Voor het beheer van gebruikers selecteert u een of meer van de volgende instellingen:

- Als u gebruikers wilt toevoegen, klikt u op **Add** (Toevoegen).
- Als u een gebruiker wilt verwijderen, klikt u op de gebruiker en klikt u vervolgens op **Delete** (Verwijderen).
- Als u vingerafdrukken wilt registreren of extra referenties voor de gebruiker wilt instellen, klikt u op de gebruiker en klikt u vervolgens op **Enroll** (Registreren).
- Als u de beleidsregels voor een specifieke gebruiker wilt bekijken, selecteert u de gebruiker en bekijkt u het beleid in het onderste venster.

Apparaatinstellingen opgeven

Binnen de applicatie Device (Apparaat) kunt u de instellingen opgeven die beschikbaar zijn voor geïntegreerde of aangesloten beveiligingsapparaten die door HP ProtectTools Security Manager worden herkend.

Vingerafdrukken

De pagina Fingerprints (Vingerafdrukken) bestaat uit drie tabbladen: Enrollment (Registratie), Sensitivity (Gevoeligheid) en Advanced (Geavanceerd).

Enrollment (Registratie)

U kunt het minimale en maximale aantal vingerafdrukken opgeven dat een gebruiker mag registreren.

U kunt ook alle gegevens van de vingerafdruklezer wissen.

△ **VOORZICHTIG:** wanneer u alle gegevens van de vingerafdruklezer wist, worden alle vingerafdrukgegevens voor alle gebruikers gewist, met inbegrip van beheerders. Als op grond van het aanmeldbeleid alleen vingerafdrukken vereist zijn, is het mogelijk dat geen enkele gebruiker zich nog kan aanmelden bij de computer.

Sensitivity (Gevoeligheid)

Verplaats de schuifregelaar om de gevoeligheid aan te passen waarmee de vingerafdrukken worden gescand.

Als uw vingerafdruk niet consistent wordt herkend, kan het beter zijn een lagere gevoeligheid in te stellen. Bij een hogere instelling is de lezer gevoeliger voor verschillen in de scans, waardoor het risico op onterechte acceptatie wordt beperkt. De instelling Medium-High (Middelhoog) geeft een goed evenwicht tussen beveiliging en gemak.

Advanced (Geavanceerd)

U kunt de vingerafdruklezer zodanig configureren dat energie wordt bespaard wanneer de computer op accuvoeding werkt.

Smartcard

U kunt de computer zodanig configureren dat de computer automatisch wordt vergrendeld zodra een smartcard wordt verwijderd. De computer wordt echter alleen vergrendeld als de smartcard tijdens de aanmelding bij Windows als verificatiereferentie is gebruikt. Wanneer een smartcard wordt verwijderd die niet is gebruikt om een gebruiker aan te melden bij Windows, wordt de computer niet vergrendeld.

▲ Schakel het selectievakje in om de vergrendeling bij het verwijderen van een smartcard in of uit te schakelen.

Gezicht

U kunt het beveiligingsniveau voor gezichtsherkenning instellen voor het juiste evenwicht tussen het gebruiksgemak en de moeilijkheid om de beveiliging van de computer te omzeilen.

1. Klik achtereenvolgens op **Start**, **Alle programma's**, **HP** en **HP ProtectTools Administrative Console**.
2. Klik op **Devices** (Apparaten) en daarna op **Face** (Gezicht).

3. Verplaats (door te klikken) de schuifregelaar naar links voor meer gebruiksgemak of verplaats de schuifregelaar naar rechts voor meer nauwkeurigheid.

   - **Convenience** (Gemak): om het voor geregistreerde gebruikers makkelijker te maken toegang te krijgen in situaties die er qua veiligheid niet toe doen, verplaatst u de schuifregelaar naar de positie **Convenience** (Gemak).
   - **Balance** (Balans): om een goed compromis te bereiken tussen beveiliging en bruikbaarheid, of als u gevoelige informatie heeft of als uw computer zich op een plek bevindt waar aanmelding door onbevoegden mogelijk is, verplaatst u de schuifregelaar naar de positie **Balance** (Balans).
   - **Accuracy** (Nauwkeurigheid): om het voor gebruikers moeilijker te maken toegang te krijgen als geregistreerde scènes of de lichtomstandigheden minder goed zijn dan normaal en het minder waarschijnlijk is dat een verkeerde aanmelding wordt geaccepteerd, verplaatst u de schuifregelaar naar de positie **Accuracy** (Nauwkeurigheid).

OPMERKING: het beveiligingsniveau geldt voor alle gebruikers.

4. Klik op **Apply** (Toepassen).

Geavanceerde instellingen

1. Klik achtereenvolgens op **Start**, **Alle programma's**, **HP** en **HP ProtectTools Administrative Console**.
2. Klik op **Devices** (Apparaten) en daarna op **Face** (Gezicht).
3. Klik op **Advanced** (Geavanceerd).

   - **Do not require user name for Windows logon (Geen gebruikersnaam vereist voor aanmelding bij Windows).**
     - Schakel het selectievakje in om gebruikers in staat te stellen zich bij Windows aan te melden zonder gebruikersnaam.
     - Schakel het selectievakje uit om gebruikers zich bij Windows aan te laten melden met gebruikersnaam.
   - **Enforce the use of PIN for face logon** (Pincode vereist bij aanmelding met gezichtsherkenning): schakel het selectievakje in om elke gebruiker een pincode (persoonlijk identificatienummer) te laten instellen en gebruiken voor aanmelding.
     - **Minimum length allowed for PIN** (Toegestane minimumlengte voor pincode): klik op de pijl-omhoog resp. de pijl-omlaag om het minimale aantal tekens dat is vereist voor de pincode te verhogen resp. verlagen.
     - **Maximum length allowed for PIN** (Toegestane maximumlengte voor pincode): klik op de pijl-omhoog resp. de pijl-omlaag om het maximale aantal tekens dat is toegestaan voor de pincode te verhogen resp. verlagen.
     - **Maximum retries allowed for PIN** (Maximaal aantal pogingen voor pincode): klik op de pijl-omhoog resp. de pijl-omlaag om het maximale aantal keren dat de pincode mag worden opgegeven te verhogen resp. verlagen.
4. Klik op **OK**.

5 Applicaties configureren

De groep Applicaties (Applicaties) is toegankelijk via het paneel van het menu Security Applications (Beveiligingsapplicaties) aan de linkerkant van het scherm van HP ProtectTools Administrative Console. Via het onderdeel Settings (Instellingen) kunt u de werking van de geïnstalleerde applicaties van HP ProtectTools Security Manager aanpassen.

U bewerkt als volgt de applicatie-instellingen:

1. Klik in het menu Tools (Extra) vanuit de groep **Applications** (Applicaties) op **Settings** (Instellingen).
2. Klik om een specifieke instelling in of uit te schakelen.
3. Klik op **Apply** (Toepassen) om de aangebrachte wijzigingen op te slaan.

Tabblad General (Algemeen)

De volgende instellingen zijn beschikbaar op het tabblad General (Algemeen):

- **Do not automatically launch the Setup Wizard for administrators (Setup-wizard niet automatisch starten voor beheerders)**: Selecteer deze optie om te voorkomen dat de wizard automatisch wordt geopend bij aanmelding.
- **Do not automatically launch the Getting Started wizard for users (Wizard Aan de slag niet automatisch starten voor gebruikers)**: Selecteer deze optie om te voorkomen dat de instelprocedure voor gebruikers automatisch wordt geopend bij aanmelding.

Tabblad Applications (Applicaties)

De instellingen die hier worden weergegeven, kunnen veranderen wanneer nieuwe applicaties worden toegevoegd aan Security Manager. De minimale instellingen die standaard worden weergegeven, zijn als volgt:

- **Applications status** (Status van applicaties): hiermee wordt de status voor alle applicaties weergegeven.
- **Password Manager** (Wachtwoordbeheer): hiermee schakelt u de applicatie Password Manager in voor alle gebruikers van de computer.
- **Privacy Manager** (Privacybeheer): hiermee schakelt u de applicatie Privacy Manager in voor alle gebruikers van de computer.
- **Enable the Discover more button** (Knop Meer ontdekken inschakelen): met deze optie kunnen alle gebruikers van deze computer applicaties toevoegen aan HP ProtectTools Security Manager door op de knop **[+] Discover more** ([+] Meer ontdekken) te klikken.

Als u alle applicaties wilt terugzetten op de fabrieksinstellingen, klikt u op **Restore Defaults** (Standaardinstellingen herstellen).

6 Beheerprogramma's

Er kunnen aanvullende applicaties beschikbaar zijn waarmee nieuwe beheervoorzieningen worden toegevoegd aan Security Manager. De beheerder van deze computer kan deze functie uitschakelen via de applicatie Settings (Instellingen).

Als u beheerprogramma's wilt toevoegen, klikt u op **[+] Management tools** ([+] Beheerprogramma's).

Updates en berichten

Als er een internetverbinding is, kunt u op de website van DigitalPersona http://www.digitalpersona.com/ zien of er nieuwe applicaties beschikbaar zijn of kunt u een schema voor automatische updates instellen.

1. Als u informatie wilt ontvangen over nieuwe applicaties en updates, schakelt u het selectievakje **Keep me informed about new applications and updates** (Houd mij op de hoogte van nieuwe applicaties en updates) in.
2. Om een schema voor automatische updates in te stellen, selecteert u het aantal dagen.
3. Om te controleren op updates, klikt u op **Check Now** (Nu controleren).

7 HP ProtectTools Security Manager

Met HP ProtectTools Security Manager kunt u de beveiliging van de computer aanzienlijk verbeteren.

U kunt gebruikmaken van de vooraf geladen Security Manager applicaties, alsook van extra applicaties die van het web te downloaden zijn:

- Uw aanmelding en wachtwoorden beheren
- Eenvoudig uw wachtwoord voor het besturingssysteem Windows® wijzigen
- Programmavoorkeuren instellen
- Vingerafdrukken gebruiken voor een betere beveiliging en meer gemak
- Een of meer scènes voor verificatie registreren
- Smartcard instellen voor verificatiedoeleinden
- Back-ups van uw programmagegevens maken en terugzetten
- Meer applicaties toevoegen

HP ProtectTools Security Manager openen

U kunt HP ProtectTools Security Manager op een van de volgende manieren openen:

- Klik achtereenvolgens op **Start**, **Alle programma's**, **HP** en **HP ProtectTools Security Manager**.
- Dubbelklik op het pictogram **HP ProtectTools** in het systeemvak helemaal rechts op de taakbalk.
- Klik met de rechtermuisknop op het pictogram **HP ProtectTools** en klik op **Open HP ProtectTools Security Manager** (HP ProtectTools Security Manager openen).
- Klik op de gadget **Security Manager ID Card** (Id-kaart Security Manager) op de zijbalk van Windows.
- Druk op de hotkeycombinatie ctrl+Windows+h om het menu Quick Links (Snelkoppelingen) van Security Manager te openen.

Dashboard van Security Manager gebruiken

Het dashboard van Security Manager is een centrale locatie van waaruit u gemakkelijk toegang heeft tot de voorzieningen, applicaties en instellingen van Security Manager.

▲ U opent het dashboard van Security Manager door achtereenvolgens op **Start**, **Alle programma's**, **HP** en **HP ProtectTools Security Manager** te klikken.

Het dashboard bestaat uit de volgende onderdelen:

- **ID Card** (Id-kaart): hier ziet u de Windows-gebruikersnaam en een afbeelding voor de aangemelde gebruikersaccount.
- **Security Applications** (Beveiligingsapplicaties): hier ziet u een uitvouwmenu met koppelingen voor het configureren van de volgende beveiligingscategorieën:
  - **Credential Manager**
  - **My Data (Mijn gegevens)**
- **Discover more** (Meer ontdekken): hiermee opent u een pagina met andere applicaties waarmee u uw identiteit, gegevens en communicatie nog beter kunt beveiligen.
- **Main area** (Hoofdgedeelte): hier worden applicatiespecifieke schermen weergegeven.
- **Administration** (Beheer): hiermee opent u de HP ProtectTools Administrative Console.
- **Help button** (Helpknop): hiermee geeft u informatie over het huidige scherm weer.
- **Advanced** (Geavanceerd): hiermee krijgt u toegang tot de volgende opties:
  - **Preferences** (Voorkeuren): met deze optie kunt u voorkeursinstellingen opgeven voor Security Manager.
  - **Backup and Restore** (Back-up en herstel): met deze optie kunt u een back-up van gegevens maken of terugzetten.
  - **About** (Info): hier wordt informatie over de versie van Security Manager weergegeven.

Instelprocedures

Referenties registreren

Op de pagina My Identity (Mijn identiteit) kunt u de verschillende verificatiemethoden of referenties registreren. Nadat deze zijn geregistreerd, kunt u deze methoden gebruiken om u aan te melden bij Security Manager.

Vingerafdrukken registreren

Als de computer een geïntegreerde of aangesloten vingerafdruklezer heeft, leidt de setup-wizard voor HP ProtectTools Security Manager u door de stappen om uw vingerafdrukken in te stellen of te "registreren".

1. De omtrekken van twee handen worden weergegeven. Vingers die al zijn geregistreerd, worden groen weergegeven. Klik op een vinger.

   OPMERKING: als u een eerder geregistreerde vingerafdruk wilt verwijderen, klikt u op de desbetreffende vinger.

2. Wanneer u de vinger heeft geselecteerd die u wilt registreren, wordt u gevraagd om die vinger te scannen totdat de vingerafdruk goed is geregistreerd. Een geregistreerde vinger wordt groen weergegeven.

3. U moet minimaal twee vingers registreren (bij voorkeur de wijs- of middelvinger). Herhaal stap 1 tot en met 3 voor een andere vinger.

4. Klik op **Next** (Volgende) en volg de instructies op het scherm.

OPMERKING: wanneer u vingerafdrukken registreert via de Aan de slag-procedure, worden de gegevens over de vingerafdrukken pas opgeslagen wanneer u op **Next** (Volgende) heeft geklikt. Als u de computer enige tijd inactief laat of het programma sluit, worden de wijzigingen die u heeft aangebracht **niet** opgeslagen.

Scènes registreren

U moet een of meer scènes registreren om aanmelding via gezichtsverificatie te kunnen gebruiken.

U registreert als volgt een nieuwe scène in de setup-wizard van HP ProtectTools Security Manager:

1. Klik op het pictogram **HP ProtectTools Security Manager** in de zijbalk aan de rechterkant van het scherm.

2. Geef uw Windows®-wachtwoord op en klik op **Next** (Volgende).

3. Schakel onder **Enable security features** (Veiligheidsvoorzieningen inschakelen) het selectievakje **Windows Logon Security** (Aanmeldingsbeveiliging van Windows) in en klik op **Next** (Volgende).

4. Schakel onder **Choose your credentials** (Uw referenties kiezen) het selectievakje **Face** (Gezicht) en klik op **Next** (Volgende).

5. Klik op **Enroll a new scene** (Nieuwe scène registreren).

Nadat u bent geregistreerd, kunt u ook een nieuwe scène registreren als u bij de aanmelding problemen ondervindt doordat een of meer van de volgende elementen zijn gewijzigd:

- Uw gezicht is significant veranderd sinds uw laatste registratie.
- De belichting is heel anders dan bij uw voorgaande registraties.
- U droeg een bril (of juist niet) tijdens uw laatste registratie.

OPMERKING: Als u problemen ondervindt bij het registreren van scènes, probeert u het opnieuw door dichter bij de webcam te gaan staan. Net als bij elk ander type fotografie of videografie zijn belichting en contrast uiterst belangrijk. Zorg ervoor dat de belichting voor de sessie voornamelijk op de voorgrond is gericht en niet voornamelijk op de achtergrond. Als u merkt dat de gezichtsherkenning u niet onmiddellijk verifieert, wilt u wellicht de scène opnieuw registreren met een betere belichting.

U registreert als volgt een nieuwe scène in HP ProtectTools Security Manager:

1. Klik achtereenvolgens op **Start**, **Alle programma's**, **HP** en **HP ProtectTools Security Manager**.
2. Klik op **Credentials** (Referenties) en daarna op **Face** (Gezicht).
3. Klik op **Enroll a new scene** (Nieuwe scène registreren).

Geavanceerde gebruikersinstellingen

1. Klik achtereenvolgens op **Start**, **Alle programma's** en **HP ProtectTools Security Manager**.
2. Klik op **Set up your authentication credentials** (Uw verificatiereferenties instellen) en daarna op **Face** (Gezicht).
3. Klik op de knop **Advanced** (Geavanceerd) en maak een keuze uit de volgende opties.

   a. Om het gebruik van een pincode bij gezichtsherkenning verplicht te stellen, klikt u op **Create PIN** (Pincode maken). Voer uw Windows-wachtwoord in, voer de nieuwe pincode in en bevestig deze door de code nogmaals in te voeren.

   b. Selecteer desgewenst extra instellingen. Deze instellingen gelden alleen voor de huidige gebruiker.

   - **Play sound on face recognition events (Geluid afspelen bij gezichtsherkenningsgebeurtenissen)**
     - Schakel het selectievakje in om een geluid af te spelen als gezichtsherkenning lukt of niet lukt.
     - Schakel het selectievakje uit om deze optie uit te schakelen.
   - **Prompt to update scenes when logon fails (Verzoeken om scènes bij te werken als aanmelding mislukt)**
     - Schakel het selectievakje in om de gebruiker in staat te stellen scènes bij te werken als gezichtsherkenning niet lukt. Als de verificatie de drempelwaarde "misschien" bereikt, wordt de gebruiker verzocht te beslissen of de live afbeeldingen in de "mislukte" aanmelding moeten worden ingevoegd in de huidige scène om de kans op een geslaagde aanmelding de volgende keer te vergroten.
     - Schakel het selectievakje uit om deze optie uit te schakelen.
   - **Prompt enroll a new scene when logon fails (Verzoeken om een nieuwe scène te registreren als aanmelding mislukt)**
     - Schakel het selectievakje in om de gebruiker te verzoeken een nieuwe scène te registreren als aanmelding met gezichtsherkenning niet lukt en de verificatie de drempelwaarde "misschien" niet bereikt. Hierdoor kan de kans op een geslaagde aanmelding de volgende keer groter zijn.
     - Schakel het selectievakje uit om deze optie uit te schakelen.

   c. Om een nieuwe scène te registreren, klikt u op **Enroll a new scene** (Nieuwe scène registreren) en volgt u de instructies op het scherm.

Windows-wachtwoord wijzigen

Met Security Manager kunt u uw Windows-wachtwoord gemakkelijker en sneller wijzigen dan via het Configuratiescherm van Windows.

U wijzigt als volgt uw Windows-wachtwoord:

1. Klik vanuit het dashboard van Security Manager op **Credentials** (Referenties) en klik vervolgens op **Password** (Wachtwoord).
2. Voer in het vak **Current Windows password** (Huidig Windows-wachtwoord) uw huidige wachtwoord in.
3. Typ een nieuw wachtwoord in het tekstvak **New Windows password** (Nieuw Windows-wachtwoord) en typ het vervolgens nogmaals in het tekstvak **Confirm new password** (Nieuwe wachtwoord bevestigen).
4. Klik op **Change** (Wijzigen) om uw huidige wachtwoord onmiddellijk te wijzigen in het nieuwe wachtwoord dat u heeft ingevoerd.

Smartcard instellen

Als u aanmelding met een smart card kiest en de computer een geïntegreerde of aangesloten smartcardlezer heeft, wordt u in de setup-wizard voor Security Manager gevraagd om een pincode (persoonlijk identificatienummer) voor de smartcard in te stellen.

U stelt als volgt een pincode voor de smartcard in:

1. Voer onder **Set up smart card** (Smartcard instellen) een pincode in en bevestig deze.

   U kunt uw pincode ook wijzigen. Voer uw huidige pincode in en voer vervolgens een nieuwe in.
2. Klik om door te gaan op **Next** (Volgende) en volg de instructies op het scherm.

– of –

▲ Klik vanuit het dashboard van Security Manager op **Credentials** (Referenties) en klik vervolgens op **Smart Card**.

- Een pincode voor de smartcard instellen: voer onder **Set up smart card** (Smartcard instellen) een pincode in en bevestig de pincode.
- Uw pincode wijzigen: geef uw huidige pincode op, voer een nieuwe pincode in en bevestig de nieuwe pincode.

Algemene taken

De applicaties in deze groep helpen u om diverse aspecten van uw digitale identiteit te beheren.

- **Security Manager**: hiermee maakt en beheert u snelkoppelingen, waarmee u websites en programma's kunt starten en u zich voor die websites en programma's kunt aanmelden door uw identiteit te verifiëren met uw Windows-wachtwoord, uw vingerafdruk of een smartcard.
- **Credentials** (Referenties): Geeft u de mogelijkheid om eenvoudig uw Windows-wachtwoord te wijzigen, uw vingerafdrukken te registreren of een smartcard in te stellen.

Als u applicaties wilt toevoegen, klikt u op de knop [+] **Discover more** (Meer ontdekken) linksonder op het dashboard. Het is mogelijk dat de beheerder deze knop heeft uitgeschakeld.

Password Manager

Het aanmelden bij Windows, websites en applicaties is eenvoudiger en veiliger wanneer u gebruikmaakt van Password Manager. Met deze applicatie kunt u sterkere wachtwoorden maken die u niet ergens hoeft op te schrijven of hoeft te onthouden en kunt u zich snel en eenvoudig aanmelden met behulp van een vingerafdruk, smartcard of uw Windows-wachtwoord.

In Password Manager kunt u het volgende doen:

- Aanmeldingen toevoegen, bewerken of verwijderen op het tabblad Manage (Beheren).
- Met Quick Links (Snelkoppelingen) uw standaardbrowser starten en u aanmelden bij een website of programma.
- Snelkoppelingen door middel van slepen en neerzetten ordenen in categorieën.
- In één oogopslag zien of uw wachtwoorden een beveiligingsrisico vormen en automatisch een gecompliceerd sterk wachtwoord genereren voor nieuwe websites.

Veel voorzieningen van Password Manager zijn ook beschikbaar via het Password Manager-pictogram dat wordt weergegeven wanneer het aanmeldscherm van een webpagina of programma de focus heeft. Klik op het pictogram om een contextmenu weer te geven waarin u kunt kiezen uit onder andere de opties die hierna worden beschreven.

Voor webpagina's of programma's waarvoor nog geen aanmelding is gemaakt

In het contextmenu zijn de volgende opties beschikbaar:

- **Add [somedomain.com] to the Password Manager** ([eendomein.com] toevoegen aan Password Manager): Met deze optie kunt u een aanmelding toevoegen voor het huidige aanmeldscherm.
- **Open Password Manager** (Password Manager openen): hiermee start u Password Manager.
- **Icon settings** (Pictograminstellingen): Met deze optie kunt u opgeven onder welke voorwaarden het pictogram van Password Manager wordt weergegeven.
- **Help**: hiermee geeft u de helpinformatie voor de Password Manager software weer.

Voor webpagina's of programma's waarvoor al een aanmelding is gemaakt

In het contextmenu zijn de volgende opties beschikbaar:

- **Fill in logon data** (Aanmeldingsgegevens invullen): Met deze optie worden uw aanmeldingsgegevens in de aanmeldvelden geplaatst en wordt vervolgens de pagina verzonden (als u dat heeft opgegeven toen u de aanmelding maakte of voor het laatst bewerkte).
- **Edit logon** (Aanmelding bewerken): Met deze optie kunt u uw aanmeldingsgegevens voor deze website bewerken.
- **Add a New Account** (Nieuwe account toevoegen): Met deze optie voegt u een account toe aan een aanmelding.
- **Open Password Manager** (Password Manager openen): hiermee start u de Password Manager applicatie.
- **Help**: hiermee geeft u de helpinformatie voor de Password Manager software weer.

OPMERKING: de beheerder van deze computer kan Security Manager zodanig hebben geconfigureerd dat er meer dan één referentie nodig is om uw identiteit te verifiëren.

Aanmeldingen toevoegen

U kunt eenvoudig een aanmelding voor een website of een programma toevoegen door één keer de aanmeldingsgegevens in te voeren. Nadat u dat heeft gedaan, worden de gegevens automatisch voor u ingevoerd vanuit Password Manager. U kunt deze aanmeldingen gebruiken nadat u naar de website of het programma heeft gebladerd. Ook kunt u in het menu **Logons** (Aanmeldingen) op een aanmelding klikken om de website of het programma automatisch te laten openen en u automatisch te laten aanmelden.

U voegt als volgt een aanmelding toe:

1. Open het aanmeldscherm voor een website of programma.
2. Klik op de pijl op het pictogram **Password Manager** en klik vervolgens op een van de volgende opties, afhankelijk van of het aanmeldscherm voor een website of een programma is:
   - Voor een website: Klik op **Add [domain name] to Password Manager** ([Domeinnaam] toevoegen aan Password Manager).
   - Voor een programma: Klik op **Add this logon screen to Password Manager** (Dit aanmeldscherm toevoegen aan Password Manager).
3. Voer uw aanmeldingsgegevens in. De aanmeldvelden op het scherm en de bijbehorende velden in het dialoogvenster zijn omkaderd met een brede oranje rand. U kunt dit dialoogvenster ook weergeven door op **Add Logon** (Aanmelding toevoegen) te klikken op het tabblad **Manage** (Beheren) in Password Manager. Sommige opties hangen af van de beveiligingsapparaten die op de computer zijn aangesloten. Dit geldt bijvoorbeeld voor het gebruik van de hotkey ctrl+Windows +h, het scannen van uw vingerafdruk of het plaatsen van een smartcard.
   a. Als u een aanmeldveld wilt invullen met een van de eerder opgegeven keuzes, klikt u op de pijlen rechts van het veld.
   b. Als u het wachtwoord voor deze aanmelding wilt weergeven, klikt u op **Show password** (Wachtwoord weergeven).

c. Als u de aanmeldvelden wilt laten invullen, maar de gegevens niet wilt laten verzenden, schakelt u het selectievakje **Automatically submit logon data** (Aanmeldingsgegevens automatisch verzenden) uit.

d. Klik op **OK**, klik op de verificatiemethode die u wilt gebruiken: **Fingerprints** (Vingerafdrukken), **Password** (Wachtwoord) of **Face** (Gezicht) en meld u aan met de geselecteerde verificatiemethode.

   Het plusteken wordt verwijderd uit het Password Manager pictogram om u te laten weten dat de aanmelding is gemaakt.

e. Als Password Manager de aanmeldvelden niet detecteert, klikt u op **More fields** (Meer velden).

   i. Schakel het selectievakje in voor elk veld dat voor aanmelding is vereist, en schakel het selectievakje uit voor elk veld dat niet voor aanmelding is vereist.

   ii. Als Password Manager niet alle aanmeldvelden kan detecteren, verschijnt er een bericht met de vraag of u door wilt gaan. Klik op **Yes** (Ja).

   iii. Er verschijnt een dialoogvenster waarin uw aanmeldvelden zijn ingevuld. Klik op het pictogram voor elk veld en sleep het naar het bijbehorende aanmeldveld. Klik vervolgens op de knop om u aan te melden bij de website.

   OPMERKING: nadat u de aanmeldgegevens voor een site handmatig heeft ingevoerd, moet u deze methode in de toekomst blijven gebruiken voor aanmelding bij dezelfde website.

   OPMERKING: het handmatig invoeren van aanmeldgegevens is alleen mogelijk in Internet Explorer 8.

   iv. Klik op **Close** (Sluiten).

Telkens wanneer u die website bezoekt of dat programma opent, wordt het pictogram van Password Manager weergegeven om aan te geven dat u zich kunt aanmelden met uw geregistreerde referenties.

Aanmeldingen bewerken

U bewerkt als volgt een aanmelding:

1. Open het aanmeldscherm voor een website of programma.
2. Als u een dialoogvenster wilt weergeven waarin u uw aanmeldingsgegevens kunt bewerken, klikt u op de pijl op het pictogram van **Password Manager** en klikt u vervolgens op **Edit logon** (Aanmelding bewerken). De aanmeldvelden op het scherm en de bijbehorende velden in het dialoogvenster zijn omkaderd met een brede oranje rand.

   U kunt dit dialoogvenster ook weergeven door op **Edit for the desired logon** (Bewerken voor de gewenste aanmelding) te klikken op het tabblad **Manage** (Beheren) van Password Manager.
3. Bewerk uw aanmeldingsgegevens.

   - Als u een aanmeldveld wilt invullen met een van de eerder opgegeven keuzes, klikt u op de pijlen rechts van het veld.
   - Als u aanvullende velden uit het scherm wilt toevoegen aan uw aanmelding, klikt u op **More fields** (Meer velden).

- Als u de aanmeldvelden wilt laten invullen, maar de gegevens niet wilt laten verzenden, schakelt u het selectievakje **Submit logon data** (Aanmeldingsgegevens verzenden) uit.
- Als u het wachtwoord voor deze aanmelding wilt weergeven, klikt u op **Show password** (Wachtwoord weergeven).

4. Klik op **OK**.

Menu Logons (Aanmeldingen) gebruiken

Password Manager biedt een snelle, gemakkelijke methode om de websites en programma's te starten waarvoor u aanmeldingen heeft gemaakt. Dubbelklik op de aanmelding voor een programma of website in het menu **Logons** (Aanmeldingen) of op het tabblad **Manage** (Beheren) in **Password Manager** om het aanmeldscherm te openen en vul vervolgens uw aanmeldingsgegevens in.

Wanneer u een aanmelding maakt, wordt deze automatisch toegevoegd aan het menu Logons (Aanmeldingen) in Password Manager.

U geeft als volgt het menu Logons (Aanmeldingen) weer:

1. Druk op de hotkeycombinatie voor **Password Manager**. De fabrieksinstelling is ctrl+Windows+h. Als u de hotkeycombinatie wilt wijzigen, klikt u op **Password Manager** en vervolgens op **Settings** (Instellingen).
2. Scan uw vingerafdruk (op computers met een geïntegreerde of aangesloten vingerafdruklezer).

Aanmeldingen ordenen in categorieën

U kunt uw aanmeldingen ordenen door categorieën te maken. Vervolgens sleept u uw aanmeldingen naar de gewenste categorieën.

U voegt als volgt een categorie toe:

1. Klik vanuit het dashboard van Security Manager op **Password Manager**.
2. Klik op het tabblad **Manage** (Beheren) en klik vervolgens op **Add Category** (Categorie toevoegen).
3. Voer een naam in voor de categorie.
4. Klik op **OK**.

U voegt als volgt een aanmelding toe aan een categorie:

1. Plaats de muisaanwijzer op de gewenste aanmelding.
2. Houd de linkermuisknop ingedrukt.
3. Sleep de aanmelding naar de lijst met categorieën. De categorieën worden gemarkeerd wanneer u de muis over de categorieën beweegt.
4. Laat de muisknop los wanneer de gewenste categorie is gemarkeerd.

Uw aanmeldingen worden niet verplaatst naar de categorie, maar gekopieerd naar de geselecteerde categorie. U kunt een bepaalde aanmelding toevoegen aan meerdere categorieën en u kunt al uw aanmeldingen weergeven door op **All** (Alle) te klikken.

Aanmeldingen beheren

Met Password Manager kunt u eenvoudig, vanuit één centrale locatie, de aanmeldingsgegevens beheren voor gebruikersnamen, wachtwoorden en meerdere aanmeldingsaccounts.

Uw aanmeldingen staan vermeld op het tabblad Manage (Beheren). Als er meerdere aanmeldingen zijn gemaakt voor dezelfde website, wordt elke aanmelding genoemd onder de naam van de website en met inspringing weergegeven in de lijst met aanmeldingen.

U beheert als volgt uw aanmeldingen:

Klik vanuit het dashboard van Security Manager op **Password Manager** en klik vervolgens op het tabblad **Manage** (Beheren).

- **Add a logon** (Een aanmelding toevoegen): Klik op **Add Logon** (Aanmelding toevoegen) en volg de instructies op het scherm.
- **Edit a logon** (Aanmelding bewerken): Klik op een aanmelding, klik op **Edit** (Bewerken) en wijzig vervolgens de aanmeldingsgegevens.
- **Delete a logon** (Aanmelding verwijderen): Klik op een aanmelding en klik vervolgens op **Delete** (Verwijderen).

U voegt als volgt een extra aanmelding toe voor een website of programma:

1. Open het aanmeldscherm voor de website of het programma.
2. Klik op het pictogram van **Password Manager** om het snelmenu ervan weer te geven.
3. Klik op **Add additional logon** (Extra aanmelding toevoegen) en volg de instructies op het scherm.

Wachtwoordsterkte beoordelen

Het gebruik van sterke wachtwoorden bij de aanmelding voor websites en programma's speelt een belangrijke rol bij de bescherming van uw identiteit.

Password Manager maakt het u gemakkelijk om het beveiligingsniveau te bewaken en te verbeteren, daar automatisch onmiddellijk de sterkte van de wachtwoorden wordt geanalyseerd die u gebruikt om u bij uw websites en programma's aan te melden.

Password Manager pictogram, instellingen

Met Password Manager wordt geprobeerd aanmeldschermen voor websites en programma's te herkennen. Wanneer een aanmeldscherm wordt gedetecteerd waarvoor u geen aanmelding heeft gemaakt, krijgt het Password Manager pictogram een plusteken ("+"), om aan te geven dat u een aanmelding voor het scherm kunt toevoegen.

Klik op het pijlpictogram en klik vervolgens op **Icon Settings** (Pictograminstellingen) om op te geven hoe met **Password Manager** mogelijke aanmeldwebsites moeten worden verwerkt.

- **Prompt to add logons for logon screens** (Vragen om aanmeldingen voor aanmeldschermen toe te voegen): Klik op deze optie als u wilt worden gevraagd of u een aanmelding wilt toevoegen wanneer een aanmeldscherm wordt weergegeven waarvoor nog geen aanmelding is ingesteld.
- **Exclude this screen** (Dit scherm uitsluiten): schakel dit selectievakje in als u niet wilt worden gevraagd of u een aanmelding voor dit aanmeldscherm wilt toevoegen.

Als u toegang wilt krijgen tot andere instellingen van Password Manager, klikt u op **Password Manager** en vervolgens op **Settings** (Instellingen) op het dashboard van Security Manager.

Instellingen

Voor HP ProtectTools Security Manager kunt u diverse voorkeursinstellingen opgeven:

1. **Prompt to add logons for logon screens** (Vragen om aanmeldingen voor aanmeldschermen toe te voegen): Wanneer het aanmeldscherm van een website of programma wordt gedetecteerd, wordt het Password Manager pictogram met een plusteken weergegeven, om aan te geven dat u een aanmelding voor dit scherm kunt toevoegen aan het wachtwoordarchief. Als u deze voorziening wilt uitschakelen, schakelt u in het dialoogvenster **Icon Settings** (Pictograminstellingen) het selectievakje naast **Prompt to add logons for logon screens** (Vragen om aanmeldingen voor aanmeldschermen toe te voegen) uit.

2. **Open Password Manager with ctrl+Windows+H** (Password Manager openen met ctrl+Windows +H): de standaardhotkey waarmee u het menu Quick Links (Snelkoppelingen) van Password Manager opent, is ctrl+Windows+H. Als u de hotkey wilt wijzigen, klikt u op deze optie en voert u een nieuwe toetscombinatie in. De combinaties kunnen een of meer van de volgende toetsen omvatten: ctrl, alt of shift en een letter- of cijfertoets.

3. Klik op **Apply** (Toepassen) om de wijzigingen op te slaan.

Referenties

U gebruikt de Security Manager referenties om te bevestigen dat u het echt bent. De lokale beheerder van de computer kan instellen welke referenties u kunt gebruiken om uw identiteit aan te tonen wanneer u zich aanmeldt bij uw Windows-account, websites of programma's.

Welke referenties beschikbaar zijn, is afhankelijk van de beveiligingsapparaten die in deze computer zijn geïntegreerd of daarop zijn aangesloten. Elke referentie die wordt ondersteund, wordt vermeld in de groep **My Identity, Credentials** (Mijn identiteit, Referenties).

De beschikbare referenties, de vereisten en de huidige status worden vermeld. Het kan hierbij onder andere gaan om:

- Vingerafdrukken
- Wachtwoord
- Smartcard
- Gezicht

Als u een referentie wilt registreren of wijzigen, klikt u op de koppeling en volgt u de instructies op het scherm.

Uw persoonlijke id-kaart

Aan de hand van uw unieke id-kaart wordt u geïdentificeerd als de eigenaar van deze Windows-account. Op de kaart staan uw naam en een afbeelding van uw keuze. De kaart wordt prominent linksboven aan de pagina's van Security Manager weergegeven, alsook als Windows Sidebar-gadget.

Een van de vele manieren waarop u snel toegang krijgt tot Security Manager, is door op uw id-kaart in de Windows Sidebar te klikken.

U kunt de afbeelding wijzigen en de manier waarop uw naam wordt weergegeven. Standaard worden uw volledige Windows-gebruikersnaam en de afbeelding die u tijdens de installatie van Windows heeft geselecteerd, getoond.

U wijzigt als volgt de weergegeven naam:

1. Klik vanuit het dashboard van Security Manager op het pictogram **ID Card** (Id-kaart) in de linkerbovenhoek.
2. Klik op het selectievakje met de naam die u heeft ingevoerd voor uw account in Windows. Uw Windows-gebruikersnaam voor deze account wordt weergegeven.
3. Als u deze naam wilt wijzigen, typt u de nieuwe naam en klikt u vervolgens op **Save** (Opslaan).

U wijzigt als volgt de weergegeven afbeelding:

1. Klik vanuit het dashboard van Security Manager op **ID Card** (Id-kaart) in de linkerbovenhoek.
2. Klik op **Choose picture** (Afbeelding kiezen), klik op een afbeelding en klik vervolgens op **Save** (Opslaan).

Voorkeuren instellen

Voor HP ProtectTools Security Manager kunt u diverse voorkeursinstellingen opgeven. Klik vanuit het dashboard van Security Manager op **Advanced** (Geavanceerd) en klik vervolgens op **Preferences** (Voorkeuren). De beschikbare instellingen worden weergegeven op twee tabbladen: General (Algemeen) en Fingerprint (Vingerafdruk).

General (Algemeen)

De volgende instellingen zijn beschikbaar op het tabblad General (Algemeen):

Appearance (Uiterlijk): **Show icon on the taskbar** (Pictogram op de taakbalk weergeven)

- Schakel het selectievakje in als u wilt dat het pictogram op de taakbalk wordt weergegeven.
- Schakel het selectievakje uit als u niet wilt dat het pictogram op de taakbalk wordt weergegeven.

Fingerprint (Vingerafdruk)

De volgende instellingen zijn beschikbaar op het tabblad Fingerprint (Vingerafdruk):

- **Quick Actions** (Snelacties): gebruik Quick Actions (Snelacties) om de Security Manager taak te selecteren die u wilt uitvoeren wanneer u een bepaalde toets ingedrukt houdt terwijl uw vingerafdruk wordt gescand.

  U wijst als volgt een snelactie toe aan een van de vermelde toetsen: klik op een optie **(Toets) +Vingerafdruk** en selecteer vervolgens een van de beschikbare taken in het menu.

- **Fingerprint Scan Feedback** (Terugkoppeling op vingerafdrukscan): deze optie wordt alleen weergegeven wanneer een vingerafdruklezer beschikbaar is. Gebruik deze instelling om de terugkoppeling aan te passen die wordt gegeven wanneer u uw vingerafdruk scant.

  - **Enable sound feedback** (Geluidssignaal inschakelen): er klinkt een geluidssignaal wanneer een vingerafdruk is gescand; er zijn verschillende geluiden voor specifieke programmagebeurtenissen. Op het tabblad Geluiden in het Configuratiescherm van Windows kunt u nieuwe geluiden toekennen aan deze gebeurtenissen, maar u kunt ook het geluidssignaal uitschakelen door deze optie uit te schakelen.

  - **Show scan quality feedback (Terugkoppeling op scankwaliteit weergeven)**

    Schakel het selectievakje in als u wilt dat alle scans worden weergegeven, ongeacht de kwaliteit.

    Schakel het selectievakje uit als alleen kwalitatief goede scans moeten worden weergegeven.

Back-up van uw gegevens maken en terugzetten

U wordt aangeraden regelmatig een back-up van de Security Manager gegevens te maken. Hoe vaak u een back-up van deze gegevens maakt, hangt af van hoe vaak de gegevens veranderen. Als u bijvoorbeeld dagelijks nieuwe aanmeldingen toevoegt, is het raadzaam dagelijks een back-up van de gegevens te maken.

Back-ups kunnen ook worden gebruikt om gegevens van de ene computer te migreren naar een andere computer (ook wel "importeren" en "exporteren" genoemd).

OPMERKING: met deze voorziening wordt alleen een back-up van de gegevens gemaakt.

HP ProtectTools Security Manager moet zijn geïnstalleerd op de computer waarop u de back-up wilt terugzetten voordat u de gegevens uit het back-upbestand kunt terugzetten.

U maakt als volgt een back-up van de gegevens:

1. Klik in het linkerpaneel op **Advanced** (Geavanceerd) en klik vervolgens op **Backup and Restore** (Backup en herstel).
2. Klik op **Back up data** (Back-up van gegevens maken).
3. Selecteer de modules die u wilt opnemen in de back-up. In de meeste gevallen zult u alle modules selecteren.
4. Voer een naam in voor het back-upbestand. Het bestand wordt standaard opgeslagen in de map Documenten. Klik op **Browse** (Bladeren) om een andere locatie op te geven.
5. Voer een wachtwoord in om het bestand te beveiligen.

6. Verifieer uw identiteit.
7. Klik op **Finish** (Voltooien).

U zet als volgt een back-up terug:

1. Klik in het linkerpaneel op **Advanced** (Geavanceerd) en klik vervolgens op **Backup and Restore** (Backup en herstel).
2. Klik op **Restore data** (Gegevens terugzetten).
3. Selecteer het back-upbestand dat u eerder heeft gemaakt. U kunt het pad invoeren in het beschikbare veld of u kunt op **Browse** (Bladeren) klikken.
4. Voer het wachtwoord in waarmee het bestand is beveiligd.
5. Selecteer de modules waarvan u de gegevens wilt terugzetten. In de meeste gevallen zult u alle vermelde modules selecteren.
6. Klik op **Finish** (Voltooien).

Discover more (Meer ontdekken)

Er kunnen extra applicaties beschikbaar zijn om dit programma uit te breiden met nieuwe voorzieningen.

Klik vanuit het dashboard van Security Manager op **[+] Discover more** ([+] Meer ontdekken) om naar aanvullende applicaties te bladeren.

OPMERKING: Als er linksonder op het dashboard geen koppeling **[+] Discover more** ([+] Meer ontdekken) aanwezig is, is deze uitgeschakeld door de beheerder van de computer.

Updates en berichten

1. Als u informatie wilt ontvangen over nieuwe applicaties en updates, schakelt u het selectievakje **Keep me informed about new applications and updates** (Houd mij op de hoogte van nieuwe applicaties en updates) in.
2. Om een schema voor automatische updates in te stellen, selecteert u het aantal dagen.
3. Om te controleren op updates, klikt u op **Check Now** (Nu controleren).

Status van beveiligingsapplicaties

Op de statuspagina van de Security Manager applicaties wordt de algehele status van de geïnstalleerde beveiligingsapplicaties weergegeven. Er wordt aangegeven welke applicaties zijn geconfigureerd en wat hun configuratiestatus is. Het overzicht verschijnt automatisch wanneer u het dashboard van Security Manager opent en klikt op **Check the status of the security applications** (Status van de beveiligingsapplicaties controleren), op **Security Applications** (Beveiligingsapplicaties) of op **Check Now** (Nu controleren) op het pictogram **Gadget** op de Windows Sidebar aan de rechterkant van het scherm.

8 Drive Encryption for HP ProtectTools (niet op alle modellen beschikbaar)

△ **VOORZICHTIG:** als u besluit de Drive Encryption-module te verwijderen, moet u eerst alle gecodeerde schijfeenheden decoderen. Als u dat niet doet, heeft u geen toegang meer tot de gegevens op gecodeerde schijfeenheden, tenzij u zich heeft aangemeld voor de herstelservice van Drive Encryption. U krijgt geen toegang tot de gecodeerde schijfeenheden door de Drive Encryption-module opnieuw te installeren.

Drive Encryption for HP ProtectTools biedt volledige gegevensbescherming doordat met Drive Encryption de vaste schijf van de computer wordt gecodeerd. Wanneer Drive Encryption is geactiveerd, moet u zich aanmelden op het aanmeldscherm voor Drive Encryption, dat wordt weergegeven voordat het Windows®-besturingssysteem wordt opgestart.

Met de setup-wizard voor HP ProtectTools kunnen Windows-beheerders Drive Encryption activeren, een back-up maken van de coderingssleutel, gebruikers toevoegen en verwijderen en Drive Encryption deactiveren. Raadpleeg de helpfunctie van de HP ProtectTools Security Manager voor meer informatie.

Met Drive Encryption kunnen de volgende taken worden uitgevoerd:

- Encryption Management (Coderingsbeheer)

  Afzonderlijke schijfeenheden coderen of decoderen

  OPMERKING: Alleen interne vaste schijven kunnen worden gecodeerd.

- Recovery (Herstel)
  - Back-upsleutels maken
  - Herstelactie uitvoeren

Configuratieprocedures

Drive Encryption openen

1. Klik achtereenvolgens op **Start**, **Alle programma's**, **HP** en **HP ProtectTools Administrative Console**.
2. Klik in het linkerdeelvenster op **Drive Encryption**.

Algemene taken

Drive Encryption activeren

Gebruik de setup-wizard voor HP ProtectTools om Drive Encryption te activeren.

OPMERKING: met deze wizard kunt u ook gebruikers toevoegen en verwijderen.

-of-

1. Klik achtereenvolgens op **Start**, **Alle programma's**, **HP** en **HP ProtectTools Administrative Console**.
2. Klik in het linkerdeelvenster op **Security** (Beveiliging) en klik vervolgens op **Features** (Voorzieningen).
3. Schakel het selectievakje **Drive Encryption** in en klik vervolgens op **Next** (Volgende).
4. Schakel onder **Drives to be encrypted** (Te coderen schijfeenheden) het selectievakje in voor de vaste schijf die u wilt coderen.
5. Plaats het opslagapparaat in het van toepassing zijnde slot.

   OPMERKING: als u de coderingssleutel wilt opslaan, moet u een USB-opslagapparaat met FAT32-indeling gebruiken.
6. Schakel onder **External storage device on which to save encryption key** (Extern opslagapparaat waarop u coderingssleutel wilt opslaan) het selectievakje in voor het opslagapparaat waarop u de coderingssleutel wilt opslaan.
7. Klik op **Apply** (Toepassen).

   De schijfcodering wordt gestart.

Raadpleeg de helpfunctie van de HP ProtectTools Security Manager voor meer informatie.

Drive Encryption deactiveren

Gebruik de setup-wizard voor HP ProtectTools om Drive Encryption te deactiveren. Raadpleeg de helpfunctie van de HP ProtectTools Security Manager voor meer informatie.

-of-

1. Klik achtereenvolgens op **Start**, **Alle programma's**, **HP** en **HP ProtectTools Administrative Console**.
2. Klik in het linkerdeelvenster op **Security** (Beveiliging) en klik vervolgens op **Features** (Voorzieningen).
3. Schakel het selectievakje **Drive Encryption** uit en klik vervolgens op **Apply** (Toepassen).

   De schijfdecodering wordt gestart.

Aanmelden nadat Drive Encryption is geactiveerd

Wanneer u de computer aanzet nadat Drive Encryption is geactiveerd en uw gebruikersaccount is vastgelegd, moet u zich aanmelden op het aanmeldingsscherm van Drive Encryption:

OPMERKING: als de Windows-beheerder Pre-boot Security (Beveiliging bij opstarten) in HP ProtectTools Security Manager heeft geactiveerd, meldt u zich bij de computer aan onmiddellijk nadat de computer is ingeschakeld, in plaats van op het aanmeldscherm van Drive Encryption.

1. Klik op uw gebruikersnaam en typ uw Windows-wachtwoord of uw pincode voor de Java™ Card, of scan een geregistreerde vinger.
2. Klik op **OK**.

OPMERKING: als u een herstelsleutel gebruikt om u aan te melden op het aanmeldingsscherm van Drive Encryption, wordt u tevens gevraagd om uw Windows-gebruikersnaam te selecteren en uw wachtwoord te typen op het aanmeldingsscherm van Windows.

Gegevens beschermen door de vaste schijf te coderen

Gebruik de setup-wizard voor HP ProtectTools als u uw gegevens wilt beschermen door de vaste schijf te coderen:

1. Klik in Security Manager op **Getting Started** (Aan de slag) en klik vervolgens op het pictogram **Security Manager Setup**. Er wordt een demonstratie van de voorzieningen van Security Manager gestart. (U kunt Security Manager ook starten vanaf de pagina Drive Encryption (Schijfcodering).)
2. Klik in het linkerdeelvenster op **Drive Encryption** en klik vervolgens op **Encryption Management** (Coderingsbeheer).
3. Klik op **Change Encryption** (Codering wijzigen).
4. Selecteer de schijfeenheid of schijfeenheden die u wilt coderen.

OPMERKING: u wordt ten zeerste aangeraden de vaste schijf te coderen.

Coderingsstatus weergeven

Gebruikers kunnen de coderingsstatus weergeven vanuit HP ProtectTools Security Manager.

OPMERKING: wijzigingen in de schijfcoderingsstatus moeten worden aangebracht via de HP ProtectTools Administrative Console.

1. Open **HP ProtectTools Security Manager**.
2. Klik onder **My Data** (Mijn gegevens) op **Encryption Status** (Coderingsstatus).

   Als Drive Encryption actief is, wordt voor de schijfeenheid een van de volgende statuscodes weergegeven:

   - Active (Actief)
   - Inactive (Inactief)
   - Not encrypted (Niet gecodeerd)
   - Encrypted (Gecodeerd)
   - Encrypting (Bezig met coderen)
   - Decrypting (Bezig met decoderen)

   Als de vaste schijf wordt gecodeerd of gedecodeerd, wordt op een voortgangsbalk het percentage voltooid aangegeven, met vermelding van de tijd die nodig is om het volledige proces te voltooien.

Geavanceerde taken

Drive Encryption beheren (beheerderstaak)

Op de pagina Encryption Management (Coderingsbeheer) kunnen beheerders de status van de schijfcodering (actief of inactief) bekijken en wijzigen, alsook de coderingsstatus van alle vaste schijven van de computer bekijken.

- Als de status Inactief is, is Drive Encryption nog niet door de Windows-beheerder geactiveerd in HP ProtectTools Security Manager en wordt de vaste schijf niet beveiligd door middel van schijfcodering. Gebruik de setup-wizard voor HP ProtectTools Security Manager om Drive Encryption te activeren.
- Als de status Actief is, is Drive Encryption geactiveerd en geconfigureerd. De schijfeenheid heeft een van de volgende statussen:
  - Not encrypted (Niet gecodeerd)
  - Encrypted (Gecodeerd)
  - Encrypting (Bezig met coderen)
  - Decrypting (Bezig met decoderen)

Afzonderlijke schijfeenheden coderen of decoderen

Als u een of meer vaste schijven van de computer wilt coderen of een reeds gecodeerde schijfeenheid wilt decoderen, gebruikt u de voorziening Change Encryption (Codering wijzigen):

1. Open **HP ProtectTools Administrative Console**, klik op **Drive Encryption** en klik vervolgens op **Encryption Management** (Coderingsbeheer).
2. Klik op **Change Encryption** (Codering wijzigen).
3. Schakel in het dialoogvenster Change Encryption (Codering wijzigen) het selectievakje in of uit voor elke vaste schijf die u wilt coderen of decoderen en klik vervolgens op **OK**.

OPMERKING: terwijl de schijfeenheid wordt gecodeerd of gedecodeerd, wordt op de voortgangsbalk aangegeven hoe lang het nog duurt om het proces tijdens de huidige sessie te voltooien. Als tijdens de codering de computer wordt afgesloten of de slaapstand, standbystand of hibernationstand wordt geactiveerd en de computer vervolgens opnieuw wordt gestart, wordt de weergegeven resterende tijd teruggezet, maar wordt de feitelijke codering hervat op het punt waar het proces was gestopt. De weergave van de resterende tijd en de voortgang verandert sneller vanwege de voortgang die al was geboekt.

Backup en herstel (beheerderstaak)

Op de pagina Recovery (Herstel) kunnen beheerders back-ups van coderingssleutels maken en terugzetten.

Local Drive Encryption Key Backup (Back-up van coderingssleutels op lokale schijfeenheid): Met deze optie kunt u een back-up van coderingssleutels maken op verwisselbare media wanneer Drive Encryption is geactiveerd.

Back-upsleutels maken

Van de coderingssleutel voor een gecodeerde schijfeenheid kunt u als volgt een back-up maken op een verwisselbaar opslagapparaat:

△ **VOORZICHTIG:** zorg ervoor dat u het opslagapparaat met de back-upsleutel op een veilige plaats bewaart. Als u uw wachtwoord vergeet of uw Java Card kwijtraakt, kunt u namelijk alleen nog via dit opslagapparaat toegang tot de vaste schijf krijgen.

1. Open **HP ProtectTools Administrative Console**, klik op **Drive Encryption** en klik vervolgens op **Recovery** (Herstel).
2. Klik op **Backup Keys** (Back-upsleutels).
3. Schakel op de pagina Select Backup Disk (Back-upschijf selecteren) het selectievakje in voor het apparaat waarop u de back-up van de coderingssleutel wilt maken en klik vervolgens op **Next** (Volgende).
4. Lees de informatie op de volgende pagina die wordt weergegeven en klik vervolgens op **Next** (Volgende). De coderingssleutel wordt opgeslagen op het opslagapparaat dat u heeft geselecteerd.
5. Klik in het bevestigingsvenster op **Finish** (Voltooien).

Herstelactie uitvoeren

U kunt als volgt een herstelactie uitvoeren als u uw wachtwoord bent vergeten:

1. Schakel de computer in.
2. Plaats het verwisselbare opslagapparaat waarop de back-upsleutel staat.
3. Wanneer het aanmeldvenster van Drive Encryption for HP ProtectTools verschijnt, klikt u op **Cancel** (Annuleren).
4. Klik op **Options** (Opties) linksonder in het scherm en klik vervolgens op **Recovery** (Herstel).
5. Selecteer het bestand dat de back-upsleutel bevat of klik op **Browse** (Bladeren) om naar het bestand te zoeken en klik vervolgens op **Next** (Volgende).
6. Klik in het bevestigingsvenster op **OK**.

   De computer wordt gestart.

OPMERKING: u wordt ten zeerste aangeraden uw wachtwoord opnieuw in te stellen nadat u een herstelactie heeft uitgevoerd.

9 Privacy Manager for HP ProtectTools (alleen bepaalde modellen)

Privacy Manager for HP ProtectTools stelt u in staat gebruik te maken van geavanceerde aanmeldingsmethoden (verificatiemethoden) om de bron, integriteit en veiligheid van communicatie te controleren bij het gebruik van e-mail, Microsoft® Office-documenten of expresberichtprogramma's.

Privacy Manager maakt gebruik van de beveiligingsinfrastructuur die door HP ProtectTools Security Manager wordt geboden. Het gaat hierbij om de volgende beveiligde aanmeldingsmethoden:

- Vingerafdrukverificatie
- Windows®-wachtwoord
- HP ProtectTools Java™ Card

U kunt alle bovengenoemde beveiligde aanmeldingsmethoden gebruiken in Privacy Manager.

Voor Privacy Manager gelden de volgende systeemvereisten:

- HP ProtectTools Security Manager 5.00 of hoger
- Besturingssysteem Windows® 7, Windows Vista® of Windows XP
- Microsoft Outlook 2007 of Microsoft Outlook 2003
- Geldige e-mailaccount

OPMERKING: een Privacy Manager Certificate (een digitaal certificaat) moet zijn aangevraagd en geïnstalleerd vanuit Privacy Manager voordat u toegang kunt krijgen tot de beveiligingsvoorzieningen. Raadpleeg Een Privacy Manager Certificate aanvragen en installeren op pagina 48 voor informatie over het aanvragen van een Privacy Manager Certificate.

Configuratieprocedures

Privacy Manager openen

U opent Privacy Manager als volgt:

1. Klik achtereenvolgens op **Start**, **Alle programma's**, **HP** en **HP ProtectTools Security Manager**.
2. Klik op **Privacy Manager**.

-of-

Klik met de rechtermuisknop op het pictogram **HP ProtectTools** in het systeemvak helemaal rechts op de taakbalk, klik op **Privacy Manager** en klik vervolgens op **Configuration** (Configuratie).

-of-

Klik op de werkbalk van een e-mailbericht in Microsoft Outlook op de pijl-omlaag naast **Send Securely** (Beveiligd verzenden) en klik vervolgens op **Certificates** (Certificaten) of **Trusted Contacts** (Vertrouwde contactpersonen).

-of-

Klik op de werkbalk van een Microsoft Office-document op de pijl-omlaag naast **Sign and Encrypt** (Ondertekenen en coderen) en klik vervolgens op **Certificates** (Certificaten) of **Trusted Contacts** (Vertrouwde contactpersonen).

Privacy Manager Certificates beheren

Privacy Manager Certificates bieden beveiliging voor gegevens en berichten. Voor deze certificaten wordt gebruikgemaakt van een cryptografische technologie die "PKI" (Public Key Infrastructure, infrastructuur van openbare sleutels) wordt genoemd. Voor PKI moeten gebruikers cryptografiesleutels verkrijgen, alsook een Privacy Manager Certificate dat is uitgegeven door een certificeringsinstantie. In tegenstelling tot de meeste gegevenscoderings- en verificatiesoftware waarvoor slechts periodiek verificatie nodig is, moet u bij gebruik van Privacy Manager elke keer dat u een e-mailbericht of een Microsoft Office-document ondertekent, uw identiteit verifiëren met behulp van een cryptografiesleutel. Met Privacy Manager kunt u veilig belangrijke gegevens opslaan en verzenden.

U kunt de volgende taken uitvoeren:

- Een Privacy Manager Certificate aanvragen en installeren
- Details van een Privacy Manager Certificate bekijken
- Privacy Manager Certificates vernieuwen
- Instellen welk Privacy Manager Certificate standaard moet worden gebruikt als er meerdere certificaten beschikbaar zijn
- Een Privacy Manager Certificate verwijderen en intrekken (geavanceerd)

Een Privacy Manager Certificate aanvragen en installeren

Voordat u gebruik kunt maken van de voorzieningen van Privacy Manager, moet u vanuit Privacy Manager met een geldig e-mailadres een Privacy Manager Certificate aanvragen en installeren. Het e-

mailadres moet als account in Microsoft Outlook zijn ingesteld op dezelfde computer als de computer waarmee u het Privacy Manager Certificate aanvraagt.

Privacy Manager Certificate aanvragen

1. Open Privacy Manager en klik op **Certificates** (Certificaten).
2. Klik op **Request a Privacy Manager certificate** (Privacy Manager Certificate aanvragen).
3. Lees de tekst op de pagina Welcome (Welkom) en klik op **Next** (Volgende).
4. Lees de licentieovereenkomst op de pagina License Agreement (Licentieovereenkomst).
5. Zorg ervoor dat het selectievakje naast **Check here to accept the terms of this license agreement** (Schakel dit selectievakje in om de voorwaarden van deze licentieovereenkomst te accepteren) is ingeschakeld en klik vervolgens op **Next** (Volgende).
6. Voer op de pagina Your Certificate Details (Details van uw certificaat) de benodigde gegevens in en klik op **Next** (Volgende).
7. Klik op de pagina "Certificate Request Accepted" (Certificaataanvraag geaccepteerd) op **Finish** (Voltooien).
8. Klik op **OK** om het certificaat te sluiten.

U ontvangt in Microsoft Outlook een e-mail met het Privacy Manager Certificate als bijlage.

Vooraf toegekend Privacy Manager Corporate Certificate verkrijgen

1. Open in Outlook het e-mailbericht waarin wordt aangegeven dat er vooraf een Corporate Certificate aan u is toegekend.
2. Klik op **Obtain** (Verkrijgen).
3. U ontvangt in Microsoft Outlook een e-mail met het Privacy Manager Certificate als bijlage.
4. Raadpleeg Privacy Manager Certificate installeren op pagina 49 om het certificaat te installeren.

Privacy Manager Certificate installeren

1. Wanneer u het e-mailbericht met uw Privacy Manager Certificate heeft ontvangen, opent u het e-mailbericht en klikt u op **Setup** (Instellen) rechtsonder in het bericht (in Outlook 2007) of linksbovenin (in Outlook 2003).
2. Voer de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.
3. Klik op de pagina Certificate Installed (Certificaat geïnstalleerd) op **Next** (Volgende).
4. Voer op de pagina Certificate Backup (Certificaatback-up) een locatie en naam voor het back-upbestand in of klik op **Browse** (Bladeren) om naar een locatie te zoeken.

   △ **VOORZICHTIG:** zorg ervoor dat u het bestand opslaat op een andere locatie dan de vaste schijf en bewaar het op een veilige plaats. Dit bestand is alleen voor uw eigen gebruik bedoeld en is nodig voor het geval u uw Privacy Manager Certificate en de bijbehorende sleutels moet herstellen.

5. Voer een wachtwoord in, bevestig het wachtwoord en klik op **Next** (Volgende).

6. Voer de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.

7. Als u vertrouwde contactpersonen wilt gaan uitnodigen, volgt u de instructies op het scherm vanaf stap 2 van het onderwerp Vertrouwde contactpersonen toevoegen op basis van Microsoft Outlook-contactpersonen op pagina 53.

   -of-

   Als u op **Cancel** (Annuleren) klikt, raadpleegt u Vertrouwde contactpersoon toevoegen op pagina 52 voor informatie over hoe u op een later tijdstip een vertrouwde contactpersoon toevoegt.

Details van een Privacy Manager Certificate bekijken

1. Open Privacy Manager en klik op **Certificates** (Certificaten).
2. Klik op een Privacy Manager Certificate.
3. Klik op **Certificate details** (Details van certificaat).
4. Klik op **OK** wanneer u de details heeft bekeken.

Privacy Manager Certificate vernieuwen

Vlak voordat het Privacy Manager Certificate vervalt, krijgt u bericht dat u het certificaat moet vernieuwen:

1. Open Privacy Manager en klik op **Certificates** (Certificaten).
2. Klik op **Renew certificate** (Certificaat vernieuwen).
3. Volg de instructies op het scherm om een nieuw Privacy Manager Certificate aan te schaffen.

OPMERKING: wanneer u een Privacy Manager Certificate vernieuwt, wordt uw oude Privacy Manager Certificate niet vervangen. U kunt een nieuw Privacy Manager Certificate aanschaffen en installeren volgens dezelfde procedures als in Een Privacy Manager Certificate aanvragen en installeren op pagina 48.

Privacy Manager Certificate als standaardcertificaat instellen

Vanuit Privacy Manager zijn alleen Privacy Manager Certificates zichtbaar, zelfs als er ook certificaten van andere certificeringsinstanties op de computer zijn geïnstalleerd.

Als op de computer meer dan één Privacy Manager Certificate staat dat vanuit Privacy Manager is geïnstalleerd, kunt u opgeven welk certificaat u als standaardcertificaat wilt gebruiken:

1. Open Privacy Manager en klik op **Certificates** (Certificaten).
2. Klik op het Privacy Manager Certificate dat u als standaardcertificaat wilt gebruiken en klik vervolgens op **Set default** (Instellen als standaard).
3. Klik op **OK**.

OPMERKING: u bent niet verplicht om het standaard-Privacy Manager Certificate te gebruiken. Vanuit de verschillende Privacy Manager voorzieningen kunt u elk gewenst Privacy Manager Certificate selecteren om te gebruiken.

Privacy Manager Certificate verwijderen

Als u een Privacy Manager Certificate verwijdert, kunt u de bestanden of gegevens die u met dat certificaat heeft gecodeerd, niet meer openen of bekijken. Als u per ongeluk een Privacy Manager Certificate heeft verwijderd, kunt u het herstellen met het back-upbestand dat u heeft gemaakt toen u het certificaat installeerde. Raadpleeg Privacy Manager Certificate herstellen op pagina 51 voor meer informatie.

U verwijdert als volgt een Privacy Manager Certificate:

1. Open Privacy Manager en klik op **Certificates** (Certificaten).
2. Klik op het Privacy Manager Certificate dat u wilt verwijderen en klik vervolgens op **Advanced** (Geavanceerd).
3. Klik op **Delete** (Verwijderen).
4. Klik in het bevestigingsvenster op **Yes** (Ja).
5. Klik op **Close** (Sluiten) en klik vervolgens op **Apply** (Toepassen).

Privacy Manager Certificate herstellen

Tijdens de installatie van het Privacy Manager Certificate maakt u een back-up van het certificaat. U kunt echter ook een back-up maken via de pagina "Migration" (Migratie). Dit back-upexemplaar kan worden gebruikt wanneer u overstapt op een andere computer of als u een certificaat op dezelfde computer wilt herstellen.

1. Open Privacy Manager en klik op **Migration** (Migratie).
2. Klik op **Restore** (Herstellen).
3. Klik op de pagina Migration File (Migratiebestand) op **Browse** (Bladeren) om het .dppsm-bestand te zoeken dat u tijdens het back-upproces heeft gemaakt en klik vervolgens op **Next** (Volgende).
4. Voer het wachtwoord in dat u heeft gebruikt toen u de back-up maakte en klik op **Next** (Volgende).
5. Klik op **Finish** (Voltooien).
6. Klik op **OK**.

Raadpleeg Privacy Manager Certificate installeren op pagina 49 of Back-up maken van Privacy Manager Certificates en vertrouwde contactpersonen op pagina 67 voor meer informatie.

Privacy Manager Certificate intrekken

Als u het vermoeden heeft dat de beveiliging van uw Privacy Manager Certificate in gevaar is gekomen, kunt u uw eigen certificaat intrekken:

OPMERKING: een ingetrokken Privacy Manager Certificate wordt niet verwijderd. Het certificaat kan nog steeds worden gebruikt om gecodeerde bestanden weer te geven.

1. Open Privacy Manager en klik op **Certificates** (Certificaten).
2. Klik op **Advanced** (Geavanceerd).
3. Klik op het Privacy Manager Certificate dat u wilt intrekken en klik vervolgens op **Revoke** (Intrekken).

4. Klik in het bevestigingsvenster op **Yes** (Ja).
5. Voer de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.
6. Volg de instructies op het scherm.

Vertrouwde contactpersonen beheren

Vertrouwde contactpersonen zijn gebruikers met wie u Privacy Manager Certificates heeft uitgewisseld, zodat u veilig met elkaar kunt communiceren.

Met het onderdeel Trusted Contacts Manager (Vertrouwde contactpersonen beheren) kunt u de volgende taken uitvoeren:

- Details van vertrouwde contactpersonen weergeven
- Vertrouwde contactpersonen verwijderen
- Intrekkingsstatus voor vertrouwde contactpersonen controleren (geavanceerd)

Vertrouwde contactpersonen toevoegen

Het toevoegen van vertrouwde contactpersonen bestaat uit drie stappen:

1. U stuurt iemand via e-mail een uitnodiging om vertrouwde geadresseerde te worden.
2. De geadresseerde reageert op de e-mail.
3. U ontvangt de e-mailreactie van de geadresseerde en u klikt op **Accept** (Accepteren).

U kunt afzonderlijke geadresseerden een e-mailuitnodiging sturen om een vertrouwde contactpersoon te worden of u kunt de uitnodiging versturen naar alle contactpersonen in uw Microsoft Outlook-adresboek.

Raadpleeg de volgende gedeelten als u vertrouwde contactpersonen wilt toevoegen.

OPMERKING: geadresseerden kunnen alleen reageren op uw uitnodiging om een vertrouwde contactpersoon te worden als Privacy Manager of de alternatieve client op hun computer is geïnstalleerd. Ga naar de website van DigitalPersona op http://DigitalPersona.com/PrivacyManager voor informatie over het installeren van de alternatieve client.

Vertrouwde contactpersoon toevoegen

1. Open Privacy Manager, klik op **Trusted Contacts Manager** (Vertrouwde contactpersonen beheren) en klik vervolgens op **Invite Contacts** (Contactpersonen uitnodigen).

   -of-

   Klik in Microsoft Outlook op de pijl-omlaag naast **Send Securely** (Beveiligd verzenden) op de werkbalk en klik vervolgens op **Invite Contacts** (Contactpersonen uitnodigen).

2. Als het dialoogvenster Select Certificate (Certificaat selecteren) wordt geopend, klikt u op het Privacy Manager Certificate dat u wilt gebruiken en klikt u vervolgens op **OK**.
3. Wanneer het dialoogvenster Trusted Contact Invitation (Uitnodiging vertrouwde contactpersoon) wordt geopend, leest u de tekst en klikt u vervolgens op **OK**.

   Er wordt automatisch een e-mail gegenereerd.

4. Voer de e-mailadressen in van degenen die u als vertrouwde contactpersonen wilt toevoegen.
5. Bewerk de tekst en zet uw naam (optioneel).
6. Klik op **Send** (Verzenden).

OPMERKING: als u geen Privacy Manager Certificate heeft verkregen, krijgt u bericht dat u alleen een uitnodiging kunt versturen als u over een Privacy Manager Certificate beschikt. Klik op **OK** om de Certificate Request Wizard (Wizard Certificaat aanvragen) te starten. Raadpleeg Een Privacy Manager Certificate aanvragen en installeren op pagina 48 voor meer informatie.

7. Voer de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.

OPMERKING: bij ontvangst van de e-mailuitnodiging moet de geadresseerde de e-mail openen, rechtsonder in de e-mail op **Accept** (Accepteren) klikken en vervolgens in het bevestigingsvenster op **OK** klikken.

8. Wanneer u via e-mail bericht krijgt dat de geadresseerde de uitnodiging accepteert, klikt u op **Accept** (Accepteren) rechtsonder in de e-mail.

   Er wordt een dialoogvenster geopend met een bevestiging dat de geadresseerde is toegevoegd aan uw lijst met vertrouwde contactpersonen.
9. Klik op **OK**.

Vertrouwde contactpersonen toevoegen op basis van Microsoft Outlook-contactpersonen

1. Open Privacy Manager, klik op **Trusted Contacts Manager** (Vertrouwde contactpersonen beheren) en klik vervolgens op **Invite Contacts** (Contactpersonen uitnodigen).

   -of-

   Klik in Microsoft Outlook op de pijl-omlaag naast **Send Securely** (Beveiligd verzenden) op de werkbalk en klik vervolgens op **Invite All My Outlook Contacts** (Al mijn Outlook-contactpersonen uitnodigen).
2. Wanneer de pagina Trusted Contact Invitation (Uitnodiging vertrouwde contactpersoon) wordt geopend, selecteert u het e-mailadres van degenen die u als vertrouwde contactpersonen wilt toevoegen en klikt u op **Next** (Volgende).
3. Wanneer de pagina Sending Invitation (Uitnodiging wordt verzonden) wordt geopend, klikt u op **Finish** (Voltooien).

   Er wordt automatisch een e-mail gegenereerd met een lijst van de geselecteerde e-mailadressen uit Microsoft Outlook.
4. Bewerk de tekst en zet uw naam (optioneel).
5. Klik op **Send** (Verzenden).

OPMERKING: als u geen Privacy Manager Certificate heeft verkregen, krijgt u bericht dat u alleen een uitnodiging kunt versturen als u over een Privacy Manager Certificate beschikt. Klik op **OK** om de Certificate Request Wizard (Wizard Certificaat aanvragen) te starten. Raadpleeg Een Privacy Manager Certificate aanvragen en installeren op pagina 48 voor meer informatie.

6. Voer de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.

OPMERKING: bij ontvangst van de e-mailuitnodiging moet de geadresseerde de e-mail openen, rechtsonder in de e-mail op **Accept** (Accepteren) klikken en vervolgens in het bevestigingsvenster op **OK** klikken.

7. Wanneer u via e-mail bericht krijgt dat de geadresseerde de uitnodiging accepteert, klikt u op **Accept** (Accepteren) rechtsonder in de e-mail.

   Er wordt een dialoogvenster geopend met een bevestiging dat de geadresseerde is toegevoegd aan uw lijst met vertrouwde contactpersonen.

8. Klik op **OK**.

Details van vertrouwde contactpersonen weergeven

1. Open Privacy Manager en klik op **Trusted Contacts** (Vertrouwde contactpersonen).
2. Klik op een vertrouwde contactpersoon.
3. Klik op **Contact details** (Details van contactpersoon).
4. Klik op **OK** wanneer u de details heeft bekeken.

Vertrouwde contactpersoon verwijderen

1. Open Privacy Manager en klik op **Trusted Contacts** (Vertrouwde contactpersonen).
2. Klik op de vertrouwde contactpersoon die u wilt verwijderen.
3. Klik op **Delete contact** (Contactpersoon verwijderen).
4. Klik in het bevestigingsvenster op **Yes** (Ja).

Intrekkingsstatus voor een vertrouwde contactpersoon controleren

U kunt als volgt controleren of een vertrouwde contactpersoon zijn of haar Privacy Manager Certificate heeft ingetrokken:

1. Open Privacy Manager en klik op **Trusted Contacts** (Vertrouwde contactpersonen).
2. Klik op een vertrouwde contactpersoon.
3. Klik op **Advanced** (Geavanceerd).

   Het dialoogvenster Advanced Trusted Contact Management (Vertrouwde contactpersonen beheren - geavanceerd) wordt geopend.

4. Klik op **Check Revocation** (Intrekking controleren).
5. Klik op **Close** (Sluiten).

Algemene taken

Privacy Manager kan worden gebruikt met de volgende Microsoft-producten:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Privacy Manager gebruiken in Microsoft Outlook

Wanneer Privacy Manager is geïnstalleerd, wordt op de werkbalk van Microsoft Outlook een knop Privacy weergegeven en wordt op de werkbalk van elk e-mailbericht in Microsoft Outlook de knop Send Securely (Beveiligd verzenden) weergegeven. Wanneer u op de pijl-omlaag naast **Privacy** of **Send Securely** (Beveiligd verzenden) klikt, zijn de volgende opties beschikbaar:

- Sign and Send (Ondertekenen en verzenden) (alleen knop Send Securely (Beveiligd verzenden)): met deze optie wordt een digitale handtekening toegevoegd aan de e-mail en wordt de e-mail verzonden nadat u uw identiteit heeft geverifieerd met de door u gekozen beveiligingsaanmeldmethode.
- Seal for Trusted Contacts and Send (Verzegelen voor vertrouwde contactpersonen en verzenden) (alleen knop Send Securely (Beveiligd verzenden)): met deze optie wordt een digitale handtekening toegevoegd aan de e-mail, wordt de e-mail gecodeerd en vervolgens verzonden nadat u uw identiteit heeft geverifieerd met de door u gekozen beveiligingsaanmeldmethode.
- Invite Contacts (Contactpersonen uitnodigen): Met deze optie kunt u iemand uitnodigen om vertrouwde contactpersoon te worden. Raadpleeg Vertrouwde contactpersoon toevoegen op pagina 52 voor meer informatie.
- Invite Outlook Contacts (Outlook-contactpersonen uitnodigen): Met deze optie kunt u alle contactpersonen in uw Microsoft Outlook-adresboek uitnodigen om vertrouwde contactpersoon te worden. Raadpleeg Vertrouwde contactpersonen toevoegen op basis van Microsoft Outlook-contactpersonen op pagina 53 voor meer informatie.
- Open the Privacy Manager software (Privacy Manager software openen): Met de opties Certificates (Certificaten), Trusted Contacts (Vertrouwde contactpersonen) en Settings (Instellingen) kunt u de Privacy Manager software openen om instellingen toe te voegen, weer te geven of te wijzigen. Raadpleeg Privacy Manager configureren voor Microsoft Outlook op pagina 55 voor meer informatie.

Privacy Manager configureren voor Microsoft Outlook

1. Open Privacy Manager, klik op **Settings** (Instellingen) en klik vervolgens op het tabblad **E-mail**.

   -of-

   Klik op de hoofdwerkbalk van Microsoft Outlook op de pijl-omlaag naast **Send Securely** (Beveiligd verzenden) (**Privacy** in Outlook 2003) en klik vervolgens op **Settings** (Instellingen).

   -of-

   Klik op de werkbalk van een Microsoft-e-mailbericht op de pijl-omlaag naast **Send Securely** (Beveiligd verzenden) en klik vervolgens op **Settings** (Instellingen).

2. Selecteer de acties die u wilt uitvoeren wanneer u een beveiligde e-mail verstuurt en klik vervolgens op **OK**.

E-mailbericht ondertekenen en verzenden

1. Klik in Microsoft Outlook op **New** (Nieuw) of **Reply** (Beantwoorden).
2. Typ uw e-mailbericht.
3. Klik op de pijl-omlaag naast **Send Securely** (Beveiligd verzenden) (**Privacy** in Outlook 2003) en klik vervolgens op **Sign and Send** (Ondertekenen en verzenden).
4. Voer de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.

E-mailbericht verzegelen en verzenden

Verzegelde e-mailberichten die digitaal zijn ondertekend en verzegeld (gecodeerd) kunnen alleen worden bekeken door mensen die u uit uw lijst met vertrouwde contactpersonen kiest.

U kunt als volgt een e-mailbericht verzegelen en verzenden naar een vertrouwde contactpersoon:

1. Klik in Microsoft Outlook op **New** (Nieuw) of **Reply** (Beantwoorden).
2. Typ uw e-mailbericht.
3. Klik op de pijl-omlaag naast **Send Securely** (Beveiligd verzenden) (**Privacy** in Outlook 2003) en klik vervolgens op **Seal for Trusted Contacts and Send** (Verzegelen voor vertrouwde contactpersonen en verzenden).
4. Voer de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.

Verzegeld e-mailbericht weergeven

Wanneer u een verzegeld e-mailbericht opent, wordt in de kop van de e-mail het beveiligingslabel weergegeven. Op het beveiligingslabel staat de volgende informatie:

- Welke referenties zijn gebruikt om de identiteit te verifiëren van degene die de e-mail heeft ondertekend
- Welk product is gebruikt om de referenties te verifiëren van degene die de e-mail heeft ondertekend

Privacy Manager gebruiken in een Microsoft Office 2007-document

OPMERKING: Privacy Manager kan alleen worden gebruikt met Microsoft Office 2007-documenten.

Nadat u uw Privacy Manager Certificate heeft geïnstalleerd, wordt in alle Microsoft Word-, Microsoft Excel- en Microsoft PowerPoint-documenten rechts op de werkbalk een knop Sign and Encrypt (Ondertekenen en coderen) weergegeven. Wanneer u op de pijl-omlaag naast **Sign and Encrypt** (Ondertekenen en coderen) klikt, kunt u kiezen uit de volgende opties:

- Sign Document (Document ondertekenen): Met deze optie wordt uw digitale handtekening toegevoegd aan het document.
- Add Signature Line Before Signing (Handtekeningregel toevoegen alvorens te ondertekenen) (alleen in Microsoft Word en Microsoft Excel): Standaard wordt een handtekeningregel toegevoegd wanneer een Microsoft Word- of Microsoft Excel-document wordt ondertekend of gecodeerd. Als u deze optie wilt uitschakelen, klikt u op **Add Signature Line** (Handtekeningregel toevoegen) om het vinkje weg te halen.
- Encrypt Document (Document coderen): Met deze optie wordt uw digitale handtekening toegevoegd en wordt het document gecodeerd.

- Remove Encryption (Codering verwijderen): Met deze optie wordt de codering van het document verwijderd.
- Open the Privacy Manager software (Privacy Manager software openen): Met de opties Certificates (Certificaten), Trusted Contacts (Vertrouwde contactpersonen) en Settings (Instellingen) kunt u de Privacy Manager software openen om instellingen toe te voegen, weer te geven of te wijzigen. Raadpleeg Privacy Manager Certificates beheren op pagina 48, Vertrouwde contactpersonen beheren op pagina 52 of Privacy Manager configureren voor Microsoft Office op pagina 57 voor meer informatie.

Privacy Manager configureren voor Microsoft Office

1. Open Privacy Manager, klik op **Settings** (Instellingen) en klik vervolgens op het tabblad **Documents** (Documenten).

   -of-

   Klik op de werkbalk van een Microsoft Office-document op de pijl-omlaag naast **Sign and Encrypt** (Ondertekenen en coderen) en klik vervolgens op **Settings** (Instellingen).

2. Selecteer de acties die u wilt configureren en klik vervolgens op **OK**.

Microsoft Office-document ondertekenen

1. Maak in Microsoft Word, Microsoft Excel of Microsoft PowerPoint een document en sla het op.
2. Klik op de pijl-omlaag naast **Sign and Encrypt** (Ondertekenen en coderen) en klik vervolgens op **Sign Document** (Document ondertekenen).
3. Voer de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.
4. Lees in het bevestigingsvenster de tekst en klik vervolgens op **OK**.

U kunt het document later als volgt bewerken:

1. Klik op **Office** linksboven aan het scherm.
2. Klik op **Prepare** (Voorbereiden) en klik vervolgens op **Mark as Final** (Markeren als definitief).
3. Klik in het bevestigingsvenster op **Yes** (Ja) en breng de gewenste bewerkingen aan.
4. Wanneer u het document naar wens heeft bewerkt, ondertekent u het document opnieuw.

Handtekeningregel toevoegen bij ondertekening van een Microsoft Word- of Microsoft Excel-document

Met Privacy Manager kunt u een handtekeningregel toevoegen wanneer u een Microsoft Word- of Microsoft Excel-document ondertekent:

1. Maak in Microsoft Word of Microsoft Excel een document en sla het op.
2. Klik op het menu **Home** (Start).
3. Klik op de pijl-omlaag naast **Sign and Encrypt** (Ondertekenen en coderen) en klik vervolgens op **Add Signature Line Before Signing** (Handtekeningregel toevoegen alvorens te ondertekenen).

OPMERKING: wanneer deze optie is geselecteerd, wordt naast de optie een vinkje weergegeven. Deze optie is standaard ingeschakeld.

4. Klik op de pijl-omlaag naast **Sign and Encrypt** (Ondertekenen en coderen) en klik vervolgens op **Sign Document** (Document ondertekenen).

5. Voer de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.

Voorgestelde ondertekenaars toevoegen aan een Microsoft Word- of Microsoft Excel-document

U kunt aan een document meerdere handtekeningregels toevoegen door voorgestelde ondertekenaars aan te wijzen. Een voorgestelde ondertekenaar is een gebruiker die door de eigenaar van een Microsoft Word- of Microsoft Excel-document is aangewezen om een handtekeningregel toe te voegen aan het document. U kunt zelf een voorgestelde ondertekenaar zijn, maar ook iemand anders waarvan u wilt dat die uw document ondertekent, kan een voorgestelde ondertekenaar zijn. Als u bijvoorbeeld een document opstelt dat door alle leden van uw afdeling moet worden ondertekend, kunt u onder aan de laatste pagina van het document de handtekeningregels voor die gebruikers opnemen, met de instructie dat zij vóór een bepaalde datum moeten tekenen.

U voegt als volgt een voorgestelde ondertekenaar toe aan een Microsoft Word- of Microsoft Excel-document:

1. Maak in Microsoft Word of Microsoft Excel een document en sla het op.

2. Klik op het menu **Insert** (Invoegen).

3. Klik in de groep **Text** (Tekst) op de werkbalk op de pijl naast **Signature Line** (Handtekeningregel) en klik vervolgens op **Privacy Manager Signature Provider** (Ondertekenaar Privacy Manager).

   Het dialoogvenster Signature Setup (Handtekening instellen) wordt geopend.

4. Voer in het tekstvak onder **Suggested signer** (Voorgestelde ondertekenaar) de naam in van de voorgestelde ondertekenaar.

5. Voer in het tekstvak onder **Instructions to the signer** (Instructies voor de ondertekenaar) een bericht voor deze voorgestelde ondertekenaar in.

   OPMERKING: dit bericht wordt weergegeven in plaats van een titel en wordt hetzij verwijderd, hetzij vervangen door de titel van de gebruiker zodra het document wordt ondertekend.

6. Schakel het selectievakje **Show sign date in signature line** (Ondertekeningsdatum weergeven in handtekeningregel) in om de datum weer te geven.

7. Schakel het selectievakje **Show signer's title in signature line** (Titel van ondertekenaar weergeven in handtekeningregel) in om de titel weer te geven.

   OPMERKING: omdat de eigenaar van het document degene is die voorgestelde ondertekenaars toewijst aan zijn of haar document, kunnen voorgestelde ondertekenaars de datum en/of titel niet in de handtekeningregel weergeven als het selectievakje **Show sign date in signature line** (Ondertekeningsdatum weergeven in handtekeningregel) en/of het selectievakje **Show signer's title in signature line** (Titel van ondertekenaar weergeven in handtekeningregel) niet is ingeschakeld, ook al is dat op grond van hun eigen documentinstellingen wel mogelijk.

8. Klik op **OK**.

Handtekeningregel van voorgestelde ondertekenaar toevoegen

Wanneer voorgestelde ondertekenaars het document openen, zien zij hun naam tussen haakjes, om aan te geven dat hun handtekening vereist is.

U ondertekent het document als volgt:

1. Dubbelklik op de van toepassing zijnde handtekeningregel.
2. Voer de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.

   De handtekeningregel wordt weergegeven volgens de instellingen die zijn opgegeven door de eigenaar van het document.

Microsoft Office-document coderen

U kunt een Microsoft Office-document voor uzelf en voor vertrouwde contactpersonen coderen. Wanneer u een document codeert en sluit, kunnen u en uw vertrouwde contactpersonen (die u in de lijst selecteert) het document alleen openen nadat een identiteitscontrole heeft plaatsgevonden.

U codeert als volgt een Microsoft Office-document:

1. Maak in Microsoft Word, Microsoft Excel of Microsoft PowerPoint een document en sla het op.
2. Klik op het menu **Home** (Start).
3. Klik op de pijl-omlaag naast **Sign and Encrypt** (Ondertekenen en coderen) en klik vervolgens op **Encrypt Document** (Document coderen).

   Het dialoogvenster Select Trusted Contacts (Vertrouwde contactpersonen selecteren) wordt geopend.
4. Klik op de naam van een vertrouwde contactpersoon die het document kan openen en de inhoud ervan kan bekijken.

OPMERKING: als u meerdere vertrouwde contactpersonen wilt selecteren, houdt u de ctrl-toets ingedrukt terwijl u op de afzonderlijke namen klikt.

5. Klik op **OK**.

Als u het document later wilt bewerken, volgt u de stappen in Codering van een Microsoft Office-document verwijderen op pagina 59. Wanneer de codering is verwijderd, kunt u het document bewerken. Volg de stappen in dit gedeelte om het document weer te coderen.

Codering van een Microsoft Office-document verwijderen

Wanneer u de codering van een Microsoft Office-document verwijdert, hoeven u en uw vertrouwde contactpersonen uw identiteit niet meer te verifiëren om het document te kunnen openen en de inhoud ervan te kunnen bekijken.

U verwijdert als volgt de codering van een Microsoft Office-document:

1. Open een gecodeerd Microsoft Word-, Microsoft Excel- of Microsoft PowerPoint-document.
2. Voer de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.
3. Klik op het menu **Home** (Start).
4. Klik op de pijl-omlaag naast **Sign and Encrypt** (Ondertekenen en coderen) en klik vervolgens op **Remove Encryption** (Codering verwijderen).

Gecodeerd Microsoft Office-document verzenden

U kunt een gecodeerd Microsoft Office-document bij een e-mailbericht voegen zonder de e-mail zelf te ondertekenen of te coderen. U maakt en verzendt een e-mail met een ondertekend of gecodeerd document net zoals u een reguliere e-mail met een bijlage maakt en verzendt.

Voor optimale beveiliging wordt u echter aangeraden om de e-mail te coderen wanneer u een ondertekend of gecodeerd Microsoft Office-document bijvoegt.

U kunt als volgt een verzegelde e-mail met een bijgevoegd ondertekend en/of gecodeerd Microsoft Office-document verzenden:

1. Klik in Microsoft Outlook op **New** (Nieuw) of **Reply** (Beantwoorden).
2. Typ uw e-mailbericht.
3. Voeg het Microsoft Office-document bij.
4. Raadpleeg E-mailbericht verzegelen en verzenden op pagina 56 voor nadere instructies.

Ondertekend Microsoft Office-document weergeven

OPMERKING: u heeft geen Privacy Manager Certificate nodig om een ondertekend Microsoft Office-document te kunnen bekijken.

Wanneer een ondertekend Microsoft Office-document wordt geopend, wordt op de statusbalk onder in het documentvenster het pictogram Digital Signature (Digitale handtekening) weergegeven.

1. Klik op **Digital Signatures** (Digitale handtekeningen) om het dialoogvenster Signatures (Handtekeningen) weer te geven of te verbergen. In dit dialoogvenster staan de namen van alle gebruikers die het document hebben ondertekend en de datum waarop ze het hebben ondertekend.
2. Als u meer details over elke handtekening wilt weergeven, klikt u met de rechtermuisknop op een naam in het dialoogvenster Signatures (Handtekeningen) en selecteert u Signature Details (Details handtekening).

Gecodeerd Microsoft Office-document weergeven

Als u een gecodeerd Microsoft Office-document wilt weergeven op een andere computer, moet Privacy Manager op die computer zijn geïnstalleerd. Bovendien moet u het Privacy Manager Certificate herstellen waarmee u het bestand heeft gecodeerd.

Als vertrouwde contactpersonen een gecodeerd Microsoft Office-document willen bekijken, moeten zij over een Privacy Manager Certificate beschikken en moet Privacy Manager op hun computer zijn geïnstalleerd. Daarnaast moeten de vertrouwde contactpersonen zijn geselecteerd door de eigenaar van het gecodeerde Microsoft Office-document.

Privacy Manager gebruiken in Windows Live Messenger

Met Privacy Manager worden de volgende voorzieningen voor beveiligde communicatie toegevoegd aan Windows Live Messenger:

- **Secure chat** (Beveiligde chat): Berichten worden verzonden op basis van het SSL/TLS over XML-protocol (Secure Sockets Layer/Transport Layer Security). Dit is dezelfde technologie als voor de beveiliging van e-commerce-transacties wordt gebruikt.
- **Recipient identification** (Identificatie van geadresseerde): hiermee kunt u de aanwezigheid en identiteit van iemand verifiëren voordat u een bericht verzendt.
- **Signed messages** (Ondertekende berichten): Met deze optie kunt u uw berichten elektronisch ondertekenen. Als u deze optie inschakelt, zijn gewijzigde berichten bij ontvangst door de geadresseerde als ongeldig gemarkeerd.
- **Hide/show feature** (Voorziening verbergen/weergeven): U kunt specifieke of alle berichten in het Privacy Manager Chat venster verbergen. U kunt ook een bericht verzenden waarvan de inhoud is verborgen. Voordat het bericht wordt weergegeven, moet verificatie plaatsvinden.
- **Secure chat history** (Beveiligde chatgeschiedenis): De logboeken van uw chatsessies worden gecodeerd voordat ze worden opgeslagen en kunnen alleen na verificatie worden bekeken.
- **Automatic locking/unlocking** (Automatische vergrendeling/ontgrendeling): U kunt het Privacy Manager Chat venster vergrendelen en ontgrendelen of zo instellen dat het automatisch na een opgegeven periode van inactiviteit wordt vergrendeld.

Privacy Manager Chat sessie starten

OPMERKING: Privacy Manager Chat kan alleen worden gebruikt als beide partijen over Privacy Manager en een geïnstalleerd Privacy Manager Certificate beschikken. Raadpleeg Een Privacy Manager Certificate aanvragen en installeren op pagina 48 voor informatie over het installeren van een Privacy Manager Certificate.

1. Als u Privacy Manager Chat in Windows Live Messenger wilt starten, volgt u een van de volgende procedures:

   a. Klik met de rechtermuisknop op een online contact in Live Messenger en selecteer vervolgens **Start an Activity** (Activiteit starten).

   b. Klik op **Start Chat** (Chat starten).

   -of-

   a. Dubbelklik op een online contact in Live Messenger en selecteer het menu **See a list of activities** (Een lijst met beschikbare activiteiten bekijken).

   b. Klik op **Actie** en klik vervolgens op **Chat starten**.

   -of-

   a. Klik met de rechtermuisknop op het pictogram **ProtectTools** in het systeemvak, klik op **Privacy Manager for HP ProtectTools** en selecteer vervolgens **Start Chat** (Chat starten).

   b. Klik in Live Messenger op **Acties: Activiteit starten** en selecteer vervolgens **Privacy Manager Chat**.

OPMERKING: alle gebruikers moeten online zijn in Live Messenger en de gebruikers moeten worden weergegeven in elkaars online-venster in Live Messenger. Klik om een online gebruiker te selecteren.

Er wordt een uitnodiging verzonden naar de contactpersoon om Privacy Manager Chat te starten. Wanneer de uitgenodigde contactpersoon de uitnodiging accepteert, wordt het Privacy Manager Chat venster geopend. Als de uitgenodigde contactpersoon niet over Privacy Manager beschikt, wordt hij of zij gevraagd om het te downloaden.

2. Klik op **Start** (Starten) om een beveiligde chat te starten.

Privacy Manager configureren voor Windows Live Messenger

1. Klik in Privacy Manager Chat op **Settings** (Instellingen).

   -of-

   Klik in Privacy Manager op **Settings** (Instellingen) en klik vervolgens op het tabblad **Chat**.

   -of-

   Klik in Privacy Manager Live Messenger History Viewer (Live Messenger-geschiedenis) op **Settings** (Instellingen).

2. Als u wilt opgeven na hoeveelheid tijd de sessie moet worden vergrendeld, selecteert u een getal in de lijst **Lock session after _ minutes of activity** (Sessie vergrendelen na _ minuten activiteit).

3. Als u een geschiedenismap wilt opgeven voor uw chatsessies, klikt u op **Browse** (Bladeren) om een map te zoeken en klikt u vervolgens op **OK**.

4. Als u wilt dat uw sessies automatisch worden gecodeerd en opgeslagen wanneer u ze sluit, schakelt u het selectievakje **Automatically save secure chat history** (Automatisch beveiligde chatgeschiedenis opslaan) in.

5. Klik op **OK**.

Chatten in het Privacy Manager Chat venster

Nadat u Privacy Manager Chat heeft gestart, wordt in Windows Live Messenger een Privacy Manager Chat venster geopend. Het gebruik van Privacy Manager Chat komt overeen met het gebruik van Windows Live Messenger, behalve dat in het Privacy Manager Chat venster de volgende aanvullende voorzieningen beschikbaar zijn:

- **Save** (Opslaan): Klik op deze knop om uw chatsessie op te slaan in de map die bij de configuratie-instellingen is opgegeven. Het is ook mogelijk om Privacy Manager Chat zodanig te configureren dat elke sessie automatisch wordt opgeslagen wanneer de sessie wordt afgesloten.
- **Hide all** (Alles verbergen) en **Show all** (Alles weergeven): Klik op de van toepassing zijnde knop om de berichten in het venster Secure Communications (Beveiligde communicatie) uit te vouwen of samen te vouwen. U kunt ook afzonderlijke berichten verbergen of weergeven door op de berichtkop te klikken.
- **Are you there?** (Bent u daar?): Klik op deze knop om te verzoeken om verificatie van uw contactpersoon.
- **Lock** (Vergrendelen): klik op deze knop om het Privacy Manager Chat venster te sluiten en terug te keren naar het venster Chat Entry (Chatopzet). Om het venster Secure Communications

(Beveiligde communicatie) weer op te roepen, klikt u op **Resume the session** (De sessie hervatten) en voert u de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.

- **Send** (Verzenden): Klik op deze knop om een gecodeerd bericht te verzenden naar uw contactpersoon.
- **Send signed** (Ondertekend verzenden): Schakel dit selectievakje in om uw berichten elektronisch te ondertekenen en te coderen. Als u deze optie inschakelt, zijn gewijzigde berichten bij ontvangst door de geadresseerde als ongeldig gemarkeerd. Telkens wanneer u een ondertekend bericht verstuurt, moet u zich identificeren.
- **Send hidden** (Verborgen verzenden): Schakel dit selectievakje in om een bericht te coderen en te verzenden waarbij alleen de berichtkop wordt weergegeven. Uw contactpersoon moet zich identificeren om de inhoud van het bericht te kunnen lezen.

Chatgeschiedenis weergeven

In de Privacy Manager Chat: Live Messenger History Viewer (Live Messenger-geschiedenis) worden gecodeerde sessiebestanden van Privacy Manager Chat weergegeven. Sessies kunnen worden opgeslagen door in het Privacy Manager Chat venster op **Save** (Opslaan) te klikken of door op het tabblad Chat van Privacy Manager te configureren dat sessies automatisch worden opgeslagen. In het overzicht wordt voor elke sessie de (gecodeerde) schermnaam van de contactpersoon weergegeven, met vermelding van de datum en tijd waarop de sessie is begonnen en geëindigd. Standaard worden sessies weergegeven voor alle e-mailaccounts die zijn ingesteld. Via het menu **Display history for** (Geschiedenis weergeven voor) kunt u specifieke accounts selecteren die u wilt weergeven.

In het overzicht kunt u de volgende taken uitvoeren:

- Alle sessies onthullen op pagina 63
- Sessies voor een specifieke account onthullen op pagina 64
- Sessie-id weergeven op pagina 64
- Sessie weergeven op pagina 64
- In sessies zoeken naar specifieke tekst op pagina 65
- Sessie verwijderen op pagina 65
- Kolommen toevoegen of verwijderen op pagina 65
- Weergegeven sessies filteren op pagina 65

U start de Live Messenger History Viewer (Live Messenger-geschiedenis) als volgt:

▲ Klik in het systeemvak helemaal rechts op de taakbalk met de rechtermuisknop op **HP ProtectTools**, klik op **Privacy Manager: for HP ProtectTools** en klik vervolgens op **Live Messenger History Viewer** (Live Messenger-geschiedenis).

-of-

▲ Klik in een chatsessie op **History Viewer** (Geschiedenis) of **History** (Geschiedenis).

Alle sessies onthullen

Wanneer alle sessies worden onthuld, ziet u de gedecodeerde schermnaam van de contactpersonen voor de geselecteerde sessie(s) en alle sessies van dezelfde account.

U onthult als volgt alle opgeslagen sessies uit de chatgeschiedenis:

1. Klik in de Live Messenger History Viewer (Live Messenger-geschiedenis) met de rechtermuisknop op een sessie en selecteer vervolgens **Reveal All Sessions** (Alle sessies onthullen).
2. Voer de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.

   De schermnamen van de contactpersonen worden gedecodeerd.
3. Dubbelklik op een sessie om de inhoud ervan weer te geven.

Sessies voor een specifieke account onthullen

Wanneer een sessie wordt onthuld, ziet u de gedecodeerde schermnaam van de contactpersonen voor de geselecteerde sessie.

U onthult als volgt een specifieke sessie uit de chatgeschiedenis:

1. Klik in de Live Messenger History Viewer (Live Messenger-geschiedenis) met de rechtermuisknop op een sessie en selecteer vervolgens **Reveal Session** (Sessie onthullen).
2. Voer de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.

   De schermnaam van de contactpersonen wordt gedecodeerd.
3. Dubbelklik op de onthulde sessie om de inhoud ervan te bekijken.

OPMERKING: bij andere sessies die met hetzelfde certificaat zijn gecodeerd, staat een ontgrendelingspictogram, om aan te geven dat u ze zonder verdere verificatie kunt bekijken door te dubbelklikken op een van die sessies. Bij sessies die met een ander certificaat zijn gecodeerd, staat een vergrendelingspictogram, om aan te geven dat voor die sessies nadere verificatie vereist is voordat u de schermnamen van de contactpersonen of de inhoud ervan kunt bekijken.

Sessie-id weergeven

U geeft als volgt een sessie-id weer:

- Klik in de Live Messenger History Viewer (Live Messenger-geschiedenis) met de rechtermuisknop op een onthulde sessie en selecteer **View session ID** (Sessie-id weergeven).

Sessie weergeven

Wanneer u een sessie weergeeft, wordt het bestand geopend, zodat u het kunt bekijken. Als de sessie niet eerder is onthuld (waardoor de gedecodeerde schermnaam van de contactpersonen wordt weergegeven), wordt tegelijkertijd de sessie onthuld.

U geeft als volgt een sessie in de Live Messenger-geschiedenis weer:

1. Klik in de Live Messenger History Viewer (Live Messenger-geschiedenis) met de rechtermuisknop op een sessie en selecteer vervolgens **View** (Weergeven).
2. Voer, als hierom wordt gevraagd, de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.

   De inhoud van de sessie wordt gedecodeerd.

In sessies zoeken naar specifieke tekst

U kunt alleen zoeken naar tekst in onthulde (gedecodeerde) sessies die in het overzichtsvenster worden weergegeven. Dit zijn de sessies waarbij de schermnaam van de contactpersonen in onbewerkte tekst wordt weergegeven.

U kunt als volgt zoeken naar tekst in sessies uit de chatgeschiedenis:

1. Klik in de Live Messenger History Viewer (Live Messenger-geschiedenis) op **Search** (Zoeken).
2. Voer de zoektekst in, configureer eventueel de gewenste zoekparameters en klik vervolgens op **OK**.

   Sessies waarin de tekst voorkomt, worden gemarkeerd in het overzichtsvenster.

Sessie verwijderen

1. Selecteer een sessie in de chatgeschiedenis.
2. Klik op **Delete** (Verwijderen).

Kolommen toevoegen of verwijderen

Standaard worden de drie meest gebruikte kolommen weergegeven in de Live Messenger History Viewer (Live Messenger-geschiedenis). U kunt kolommen toevoegen aan of verwijderen uit het overzicht.

U voegt als volgt kolommen toe aan het overzicht:

1. Klik met de rechtermuisknop op een kolomkop en selecteer vervolgens **Add/Remove Columns** (Kolommen toevoegen/verwijderen).
2. Selecteer een kolomkop in het linkerpaneel en klik vervolgens op **Add** (Toevoegen) om deze naar het rechterpaneel te verplaatsen.

U verwijdert als volgt kolommen uit het overzicht:

1. Klik met de rechtermuisknop op een kolomkop en selecteer vervolgens **Add/Remove Columns** (Kolommen toevoegen/verwijderen).
2. Selecteer een kolomkop in het linkerpaneel en klik vervolgens op **Remove** (Verwijderen) om deze naar het linkerpaneel te verplaatsen.

Weergegeven sessies filteren

In de Live Messenger History Viewer (Live Messenger-geschiedenis) wordt een lijst met sessies voor al uw accounts weergegeven. U kunt de weergegeven sessies ook filteren op:

- Specifieke accounts. Raadpleeg Sessies voor een specifieke account weergeven op pagina 66 voor meer informatie.
- Datumbereik. Raadpleeg Sessies binnen een datumbereik weergeven op pagina 66 voor meer informatie.
- Andere mappen. Raadpleeg Sessies in een andere map dan de standaardmap weergeven op pagina 66 voor meer informatie.

Sessies voor een specifieke account weergeven

- Selecteer in de Live Messenger History Viewer (Live Messenger-geschiedenis) een account in het menu **Display history for** (Geschiedenis weergeven voor).

Sessies binnen een datumbereik weergeven

1. Klik in de Live Messenger History Viewer (Live Messenger-geschiedenis) op **Advanced Filter** (Geavanceerd filter).

   Het dialoogvenster Advanced Filter (Geavanceerd filter) wordt geopend.

2. Schakel het selectievakje **Display only sessions within specified date range** (Alleen sessies binnen opgegeven datumbereik weergeven) in.

3. Voer in de tekstvakken **From date** (Van datum) en **To date** (Tot datum) de dag, de maand en/of het jaar in of klik op de pijl naast de agenda om de datums te selecteren.

4. Klik op **OK**.

Sessies in een andere map dan de standaardmap weergeven

1. Klik in de Live Messenger History Viewer (Live Messenger-geschiedenis) op **Advanced Filter** (Geavanceerd filter).

2. Schakel het selectievakje **Use an alternate history files folder** (Andere map voor geschiedenisbestanden gebruiken) in.

3. Voer de maplocatie in of klik op **Browse** (Bladeren) om naar een map te zoeken.

4. Klik op **OK**.

Geavanceerde taken

Privacy Manager-certificaten en vertrouwde contactpersonen overbrengen naar een andere computer

U kunt uw Privacy Manager Certificates en vertrouwde contactpersonen veilig migreren naar een andere computer of uit veiligheidsoverwegingen een back-up maken van uw gegevens. Maak in dat geval een back-up van de gegevens, beveilig het back-upbestand met een wachtwoord, sla het bestand op een netwerklocatie of een verwisselbaar opslagapparaat op en zet het bestand tot slot over naar de nieuwe computer.

Back-up maken van Privacy Manager Certificates en vertrouwde contactpersonen

U maakt als volgt een back-up van uw Privacy Manager Certificates en vertrouwde contactpersonen in een bestand dat met een wachtwoord is beveiligd:

1. Open Privacy Manager en klik op **Migration** (Migratie).
2. Klik op **Backup** (Back-up).
3. Selecteer op de pagina Select Data (Gegevens selecteren) de gegevenscategorieën die u in het migratiebestand wilt opnemen en klik vervolgens op **Next** (Volgende).
4. Voer op de pagina Migration File (Migratiebestand) een bestandsnaam in of klik op **Browse** (Bladeren) om een locatie te zoeken en klik tot slot op **Next** (Volgende).
5. Voer een wachtwoord in, bevestig het wachtwoord en klik op **Next** (Volgende).

OPMERKING: bewaar dit wachtwoord op een veilige plaats; u heeft het nodig wanneer u het migratiebestand herstelt.

6. Voer de verificatie uit met de door u gekozen beveiligde aanmeldingsmethode.
7. Klik op de pagina Migration File Saved (Migratiebestand opgeslagen) op **Finish** (Voltooien).

Back-up van Privacy Manager Certificates en vertrouwde contactpersonen terugzetten

U zet als volgt een back-up van Privacy Manager Certificates en vertrouwde contactpersonen terug op een andere computer (bij migratie) of op dezelfde computer:

1. Open Privacy Manager en klik op **Migration** (Migratie).
2. Klik op **Restore** (Herstellen).
3. Klik op de pagina Migration File (Migratiebestand) op **Browse** (Bladeren) om een bestand te zoeken en klik vervolgens op **Next** (Volgende).
4. Voer het wachtwoord in dat u heeft gebruikt toen u het back-upbestand maakte en klik op **Next** (Volgende).
5. Klik op de pagina Migration File (Migratiebestand) op **Finish** (Voltooien).

Centraal beheer van Privacy Manager

De installatie van Privacy Manager kan zijn uitgevoerd als onderdeel van een gecentraliseerde installatie die is aangepast door de beheerder. Een of meer van de volgende voorzieningen kan zijn ingeschakeld of uitgeschakeld:

- **Certificate use policy** (Beleid voor gebruik van certificaten): Het is mogelijk dat u alleen Privacy Manager Certificates mag gebruiken die door Comodo zijn uitgegeven of dat u ook digitale certificaten mag gebruiken die door andere certificeringsinstanties zijn uitgegeven.
- **Encryption policy** (Coderingsbeleid): De coderingsmogelijkheden kunnen afzonderlijk worden ingeschakeld of uitgeschakeld in Microsoft Office of Outlook en in Windows Live Messenger.

10 File Sanitizer for HP ProtectTools

File Sanitizer is een hulpprogramma waarmee u op een veilige manier gegevenselementen (zoals persoonlijke gegevens of bestanden, geschiedenisgegevens of webgegevens) op de computer kunt versnipperen ("shredden") en periodiek de vaste schijf kunt opschonen.

OPMERKING: deze versie van File Sanitizer kan alleen voor de vaste schijf van het systeem worden gebruikt.

Versnipperen

Versnipperen (of "shredden") is iets anders dan de standaardmethode die in Windows® wordt gebruikt om items te verwijderen (in File Sanitizer ook wel "eenvoudige verwijdermethode" genoemd). Wanneer u namelijk File Sanitizer gebruikt om een item te versnipperen, wordt een algoritme aangeroepen waarmee de gegevens worden verborgen, zodat het vrijwel onmogelijk wordt om het oorspronkelijke item terug te halen. Met de eenvoudige verwijdermethode van Windows bestaat de kans dat het bestand (of het item) intact op de vaste schijf blijft staan of met forensische methoden kan worden teruggehaald.

Wanneer u een shredprofiel kiest (een profiel met hoge, gemiddelde of lage beveiliging), worden automatisch een voorafgedefinieerde lijst met gegevenselementen en een wismethode geselecteerd. U kunt ook een shredprofiel aanpassen; hierbij geeft u het aantal shredcycli op en geeft u aan op welke gegevenselementen de shredbewerking moet worden toegepast, voor welke gegevenselementen u de shredbewerking eerst wilt bevestigen en welke gegevenselementen u wilt uitsluiten van de shredbewerking. Raadpleeg Shredprofiel selecteren of maken op pagina 73 voor meer informatie.

U kunt een schema voor automatische versnippering instellen, maar ook handmatig gegevenselementen versnipperen wanneer u dat wilt. Raadpleeg Shredschema instellen op pagina 72, Eén gegevenselement handmatig versnipperen op pagina 77 of Alle geselecteerde items handmatig versnipperen op pagina 77 voor meer informatie.

OPMERKING: een .dll-bestand wordt alleen versnipperd en van het systeem verwijderd als het naar de Prullenbak is verplaatst.

Vrije ruimte schoonmaken

Wanneer een gegevenselement in Windows wordt verwijderd, wordt de inhoud van het gegevenselement niet volledig verwijderd van de vaste schijf. Alleen de verwijzing naar het gegevenselement wordt verwijderd. De inhoud van het gegevenselement blijft op de vaste schijf staan totdat dat gedeelte van de vaste schijf wordt overschreven door andere gegevens.

Bij het schoonmaken van vrije ruimte worden willekeurige gegevens over verwijderde gegevens geschreven, waardoor wordt voorkomen dat gebruikers de oorspronkelijke inhoud van de verwijderde gegevens kunnen bekijken.

OPMERKING: het schoonmaken van vrije ruimte is bedoeld voor gegevenselementen die u naar de Prullenbak van Windows verplaatst of die u handmatig verwijdert. Het schoonmaken van vrije ruimte biedt geen extra beveiliging voor versnipperde gegevenselementen.

U kunt een schema opgeven waarmee automatisch vrije ruimte wordt schoongemaakt of u kunt het proces handmatig activeren door op het pictogram **HP ProtectTools** in het systeemvak, helemaal rechts op de taakbalk, te klikken. Raadpleeg Schema instellen voor het schoonmaken van vrije ruimte op pagina 73 of Schoonmaken van vrije ruimte handmatig activeren op pagina 78 voor meer informatie.

Configuratieprocedures

File Sanitizer openen

U opent File Sanitizer als volgt:

1. Klik achtereenvolgens op **Start**, **Alle programma's**, **HP** en **HP ProtectTools Security Manager**.
2. Klik op **File Sanitizer**.

-of-

- Dubbelklik op het pictogram **File Sanitizer** op het bureaublad.

-of-

- Klik met de rechtermuisknop op het pictogram **HP ProtectTools** in het systeemvak helemaal rechts op de taakbalk, klik op **File Sanitizer** en klik vervolgens op **Open File Sanitizer** (File Sanitizer openen).

Shredschema instellen

OPMERKING: raadpleeg Shredprofiel selecteren of maken op pagina 73 voor informatie over het selecteren van een voorafgedefinieerd shredprofiel of het maken van een shredprofiel.

OPMERKING: raadpleeg Eén gegevenselement handmatig versnipperen op pagina 77 voor informatie over het handmatig versnipperen van gegevenselementen.

1. Open File Sanitizer en klik op **Shred** (Versnipperen).
2. Selecteer een shredoptie:
   - **Windows shutdown** (Afsluiten van Windows): Kies deze optie als u alle geselecteerde gegevenselementen wilt versnipperen wanneer Windows wordt afgesloten.

     OPMERKING: wanneer deze optie is geselecteerd, wordt bij het afsluiten een dialoogvenster weergegeven met de vraag of u wilt doorgaan met het versnipperen van de geselecteerde gegevenselementen of dat u de procedure wilt overslaan. Klik op **Yes** (Ja) om het versnipperen over te slaan of klik op **No** (Nee) om door te gaan zonder items te versnipperen.
   - **Web browser open** (Openen van webbrowser): Kies deze optie als u wilt dat alle geselecteerde, met het web samenhangende gegevenselementen, zoals de browsergeschiedenis, worden versnipperd wanneer u een webbrowser opent.
   - **Web browser quit** (Afsluiten van webbrowser): Kies deze optie als u wilt dat alle geselecteerde, met het web samenhangende gegevenselementen, zoals de browsergeschiedenis, worden versnipperd wanneer u een webbrowser sluit.
   - **Key sequence** (Toetsencombinatie): Kies deze optie om de versnippering te starten met een toetsencombinatie.
   - **Scheduler** (Planner): Schakel het selectievakje **Activate Scheduler** (Planner activeren) in, voer uw Windows-wachtwoord in en voer vervolgens een dag en tijdstip in waarop de geselecteerde gegevenselementen moeten worden versnipperd.

OPMERKING: een .dll-bestand wordt alleen versnipperd en van het systeem verwijderd als het naar de Prullenbak is verplaatst.

3. Klik op **Apply** (Toepassen) en daarna op **OK**.

Schema instellen voor het schoonmaken van vrije ruimte

OPMERKING: het schoonmaken van vrije ruimte is bedoeld voor gegevenselementen die u naar de Prullenbak van Windows verplaatst of die u handmatig verwijdert. Het schoonmaken van vrije ruimte biedt geen extra beveiliging voor versnipperde gegevenselementen.

U stelt als volgt een schema in voor het schoonmaken van vrije ruimte:

1. Open File Sanitizer en klik op **Free Space Bleaching** (Vrije ruimte schoonmaken).
2. Schakel het selectievakje **Activate Scheduler** (Planner activeren) in, voer uw Windows-wachtwoord in en voer vervolgens een dag en tijdstip in waarop de vrije ruimte op de vaste schijf moet worden schoongemaakt.
3. Klik op **Apply** (Toepassen) en daarna op **OK**.

OPMERKING: het schoonmaken van vrije ruimte kan veel tijd in beslag nemen. Hoewel de schoonmaakprocedure op de achtergrond wordt uitgevoerd, kan de computer trager werken als gevolg van de hogere processorbelasting.

Shredprofiel selecteren of maken

U kunt een wismethode opgeven en de gegevenselementen selecteren die u wilt versnipperen door een voorafgedefinieerd profiel te selecteren of door een eigen profiel te maken.

Voorafgedefinieerd shredprofiel selecteren

Wanneer u een voorafgedefinieerd shredprofiel kiest (een profiel met hoge, gemiddelde of lage beveiliging), worden automatisch een voorafgedefinieerde wismethode en een lijst met gegevenselementen geselecteerd. U kunt op **View Details** (Details weergeven) klikken om de voorafgedefinieerde lijst met gegevenselementen te bekijken die voor de shredbewerking zijn geselecteerd.

U selecteert als volgt een voorafgedefinieerd shredprofiel:

1. Open File Sanitizer en klik op **Settings** (Instellingen).
2. Klik op een voorafgedefinieerd shredprofiel.
3. Klik op **View Details** (Details weergeven) om de voorafgedefinieerde lijst met gegevenselementen te bekijken die voor de shredbewerking zijn geselecteerd.
4. Schakel onder **Shred the following** (De volgende items versnipperen) het selectievakje in voor elk gegevenselement waarvoor u de shredbewerking eerst wilt bevestigen.
5. Klik op **Apply** (Toepassen) en daarna op **OK**.

Shredprofiel aanpassen

Wanneer u een shredprofiel maakt, geeft u het aantal shredcycli op en geeft u aan op welke gegevenselementen de shredbewerking moet worden toegepast, voor welke gegevenselementen u de

shredbewerking eerst wilt bevestigen en welke gegevenselementen u wilt uitsluiten van de shredbewerking:

1. Open File Sanitizer en klik achtereenvolgens op **Settings** (Instellingen), **Advanced Security Settings** (Geavanceerde beveiligingsinstellingen) en **View Details** (Details weergeven).
2. Geef het aantal shredcycli op.

OPMERKING: het geselecteerde aantal shredcycli geldt voor elk gegevenselement. Als u bijvoorbeeld drie shredcycli kiest, wordt een algoritme waarmee de gegevens worden verborgen, drie afzonderlijke keren uitgevoerd. Als u een shredcyclus met een hogere beveiliging kiest, kan de shredbewerking vrij veel tijd in beslag nemen; hoe hoger het aantal shredcycli dat u opgeeft, des te kleiner echter de kans dat de gegevens kunnen worden teruggehaald.

3. Selecteer de gegevenselementen die u wilt versnipperen:
   a. Klik onder **Available shred options** (Beschikbare shredopties) op een gegevenselement en klik vervolgens op **Add** (Toevoegen).
   b. Als u een aangepast gegevenselement wilt toevoegen, klikt u op **Add Custom Option** (Aangepaste optie toevoegen) en zoekt of typt u het pad naar de bestandsnaam of de map. Klik op **Open** (Openen) en klik vervolgens op **OK**. Klik onder **Available shred options** (Beschikbare shredopties) op het aangepaste gegevenselement en klik vervolgens op **Add** (Toevoegen).

OPMERKING: als u een gegevenselement wilt verwijderen uit de beschikbare shredopties, klikt u op het gegevenselement en klikt u vervolgens op **Delete** (Verwijderen).

4. Schakel onder **Shred the following** (De volgende items versnipperen) het selectievakje in voor elk gegevenselement waarvoor u de shredbewerking eerst wilt bevestigen.

OPMERKING: als u een gegevenselement wilt verwijderen uit de shredlijst, klikt u op het gegevenselement en klikt u vervolgens op **Remove** (Verwijderen).

5. Als u bestanden of mappen wilt beschermen tegen automatische versnippering, klikt u onder **Do not shred the following** (De volgende items niet versnipperen) op **Add** (Toevoegen) en zoekt of typt u het pad naar de bestandsnaam of de map. Klik op **Open** (Openen) en klik vervolgens op **OK**.

OPMERKING: als u een gegevenselement wilt verwijderen uit de lijst met uitsluitingen, klikt u op het gegevenselement en klikt u vervolgens op **Delete** (Verwijderen).

6. Wanneer u het shredprofiel heeft geconfigureerd, klikt u op **Apply** (Toepassen) en klikt u vervolgens op **OK**.

Profiel voor eenvoudige verwijdermethode aanpassen

Met het profiel voor de eenvoudige verwijdermethode worden gegevenselementen op de standaardwijze verwijderd zonder dat ze worden versnipperd. Wanneer u een profiel voor een eenvoudige verwijdermethode aanpast, geeft u aan op welke gegevenselementen de eenvoudige verwijdermethode moet worden toegepast, voor welke gegevenselementen u de eenvoudige verwijderactie eerst wilt bevestigen en welke gegevenselementen u wilt uitsluiten van de eenvoudige verwijderactie.

OPMERKING: als u gebruikmaakt van de eenvoudige verwijdermethode, kunt u van tijd tot tijd de voorziening Vrije ruimte schoonmaken gebruiken voor de items die handmatig zijn verwijderd of naar de Prullenbak van Windows zijn verplaatst.

U past als volgt een profiel voor een eenvoudige verwijdermethode aan:

1. Open File Sanitizer en klik achtereenvolgens op **Settings** (Instellingen), **Simple Delete Setting** (Eenvoudige verwijdermethode) en **View Details** (Details weergeven).
2. Selecteer de gegevenselementen die u wilt verwijderen:
   a. Klik onder **Available delete options** (Beschikbare verwijderopties) op een gegevenselement en klik vervolgens op **Add** (Toevoegen).
   b. Als u een aangepast gegevenselement wilt toevoegen, klikt u op **Add Custom Option** (Aangepaste optie toevoegen), voert u een bestandsnaam of mapnaam in en klikt u vervolgens op **OK**. Klik op het aangepaste gegevenselement en klik op **Add** (Toevoegen).

OPMERKING: als u een gegevenselement wilt verwijderen uit de beschikbare verwijderopties, klikt u op het gegevenselement en klikt u vervolgens op **Delete** (Verwijderen).

3. Schakel onder **Delete the following** (De volgende items verwijderen) het selectievakje in voor elk gegevenselement waarvoor u de verwijderactie eerst wilt bevestigen.

OPMERKING: als u een gegevenselement wilt verwijderen uit de verwijderlijst, klikt u op het gegevenselement en klikt u vervolgens op **Remove** (Verwijderen).

4. Klik onder **Do not delete the following** (De volgende items niet verwijderen) op **Add** (Toevoegen) om de gegevenselementen te selecteren die u wilt uitsluiten van versnippering.

OPMERKING: als u een gegevenselement wilt verwijderen uit de lijst met uitsluitingen, klikt u op het gegevenselement en klikt u vervolgens op **Delete** (Verwijderen).

5. Nadat u het profiel voor de eenvoudige verwijdermethode heeft geconfigureerd, klikt u op **Apply** (Toepassen) en klikt u vervolgens op **OK**.

Algemene taken

Met File Sanitizer kunt u de volgende taken uitvoeren:

- Versnippering starten met een toetsencombinatie: U kunt de versnippering met een toetsencombinatie (bijvoorbeeld ctrl+alt+s). Raadpleeg Shredbewerking starten met een toetsencombinatie op pagina 76 voor meer informatie.
- Versnippering starten met het pictogram van File Sanitizer: Deze voorziening is vergelijkbaar met de voorziening Slepen-en-neerzetten in Windows. Raadpleeg File Sanitizer pictogram gebruiken op pagina 77 voor meer informatie.
- Een specifiek gegevenselement of alle geselecteerde gegevenselementen handmatig versnipperen: U kunt items handmatig versnipperen zonder te hoeven wachten totdat het reguliere shredschema wordt geactiveerd. Raadpleeg Eén gegevenselement handmatig versnipperen op pagina 77 of Alle geselecteerde items handmatig versnipperen op pagina 77 voor meer informatie.
- Procedure voor het schoonmaken van vrije ruimte handmatig activeren: U kunt het schoonmaken van vrije ruimte handmatig activeren. Raadpleeg Schoonmaken van vrije ruimte handmatig activeren op pagina 78 voor meer informatie.
- Shred- of schoonmaakbewerking afbreken: U kunt de shred- of schoonmaakbewerking stoppen. Raadpleeg Shred- of schoonmaakbewerking afbreken op pagina 78 voor meer informatie.
- Logboekbestanden bekijken: U kunt de logboekbestanden voor shred- en schoonmaakbewerkingen bekijken, waarin eventuele fouten of mislukte acties van de laatste shred- of schoonmaakbewerking staan vermeld. Raadpleeg Logboekbestanden weergeven op pagina 78 voor meer informatie.

OPMERKING: het versnipperen van gegevenselementen en het schoonmaken van vrije ruimte kunnen veel tijd in beslag nemen. Hoewel de shred- en schoonmaakprocedures op de achtergrond worden uitgevoerd, kan de computer trager werken als gevolg van de hogere processorbelasting.

Shredbewerking starten met een toetsencombinatie

U geeft als volgt een toetsencombinatie op:

1. Open File Sanitizer en klik op **Shred** (Versnipperen).
2. Schakel het selectievakje **Key sequence** (Toetsencombinatie) in.
3. Voer in het tekstvak een teken in.
4. Schakel het selectievakje **CTRL** of **ALT** in en schakel vervolgens het selectievakje **SHIFT** in.

   Als u bijvoorbeeld een automatische versnipperingsactie wilt starten met de s-toets en ctrl+shift, typt u de letter `s` in het tekstvak en schakelt u vervolgens de selectievakjes **CTRL** en **SHIFT** in.

   OPMERKING: zorg ervoor dat u een toetsencombinatie selecteert die anders is dan de toetsencombinaties die al zijn geconfigureerd.

U start een shredbewerking als volgt met een toetsencombinatie:

1. Houd de shift-toets en de ctrl-toets of de alt-toets (of de door u opgegeven combinatie) ingedrukt, terwijl u op het door u gekozen teken drukt.
2. Klik op **Yes** (Ja) als er een bevestigingsvenster wordt geopend.

File Sanitizer pictogram gebruiken

△ **VOORZICHTIG:** gegevenselementen die zijn versnipperd, kunnen niet worden hersteld. Ga behoedzaam te werk wanneer u items selecteert die u handmatig wilt versnipperen.

1. Navigeer naar het document of de map die u wilt versnipperen.
2. Sleep het gegevenselement naar het pictogram **File Sanitizer** op het bureaublad.
3. Klik in het bevestigingsvenster op **Yes** (Ja).

Eén gegevenselement handmatig versnipperen

△ **VOORZICHTIG:** gegevenselementen die zijn versnipperd, kunnen niet worden hersteld. Ga behoedzaam te werk wanneer u items selecteert die u handmatig wilt versnipperen.

1. Klik met de rechtermuisknop op het pictogram **HP ProtectTools** in het systeemvak helemaal rechts op de taakbalk, klik op **File Sanitizer** en klik vervolgens op **Shred One** (Eén versnipperen).
2. Wanneer het dialoogvenster Browse (Bladeren) wordt geopend, navigeert u naar het gegevenselement dat u wilt versnipperen en klikt u vervolgens op **OK**.

OPMERKING: het gegevenselement dat u selecteert, kan één bestand of map zijn.

3. Klik in het bevestigingsvenster op **Yes** (Ja).

-of-

1. Klik met de rechtermuisknop op het pictogram **File Sanitizer** op het bureaublad en klik vervolgens op **Shred One** (Eén versnipperen).
2. Wanneer het dialoogvenster Browse (Bladeren) wordt geopend, navigeert u naar het gegevenselement dat u wilt versnipperen en klikt u vervolgens op **OK**.
3. Klik in het bevestigingsvenster op **Yes** (Ja).

-of-

1. Open File Sanitizer en klik op **Shred** (Versnipperen).
2. Klik op **Browse** (Bladeren).
3. Wanneer het dialoogvenster Browse (Bladeren) wordt geopend, navigeert u naar het gegevenselement dat u wilt versnipperen en klikt u vervolgens op **OK**.
4. Klik in het bevestigingsvenster op **Yes** (Ja).

Alle geselecteerde items handmatig versnipperen

1. Klik met de rechtermuisknop op het pictogram **HP ProtectTools** in het systeemvak helemaal rechts op de taakbalk, klik op **File Sanitizer** en klik vervolgens op **Shred Now** (Nu versnipperen).
2. Klik in het bevestigingsvenster op **Yes** (Ja).

-of-

1. Klik met de rechtermuisknop op het pictogram **File Sanitizer** op het bureaublad en klik vervolgens op **Shred Now** (Nu versnipperen).
2. Klik in het bevestigingsvenster op **Yes** (Ja).

-of-

1. Open File Sanitizer en klik op **Shred** (Versnipperen).
2. Klik op **Shred Now** (Nu versnipperen).
3. Klik in het bevestigingsvenster op **Yes** (Ja).

Schoonmaken van vrije ruimte handmatig activeren

1. Klik met de rechtermuisknop op het pictogram **HP ProtectTools** in het systeemvak helemaal rechts op de taakbalk, klik op **File Sanitizer** en klik vervolgens op **Bleach Now** (Nu schoonmaken).
2. Klik in het bevestigingsvenster op **Yes** (Ja).

-of-

1. Open File Sanitizer en klik op **Free Space Bleaching** (Vrije ruimte schoonmaken).
2. Klik op **Bleach Now** (Nu schoonmaken).
3. Klik in het bevestigingsvenster op **Yes** (Ja).

Shred- of schoonmaakbewerking afbreken

Wanneer een shred- of schoonmaakbewerking aan de gang is, wordt boven het pictogram van HP ProtectTools Security Manager in het systeemvak een bericht weergegeven. Het bericht bevat details over de shred- of schoonmaakbewerking (percentage voltooid) en een optie om de bewerking af te breken.

U breekt de bewerking als volgt af:

- Klik op het bericht en klik vervolgens op **Stop** (Stoppen) als u de bewerking wilt annuleren.

Logboekbestanden weergeven

Telkens wanneer een shred- of schoonmaakbewerking wordt uitgevoerd, worden logboekbestanden van eventuele fouten of mislukte acties gegenereerd. De logboekbestanden worden altijd bijgewerkt met de laatste shred- of schoonmaakbewerking.

OPMERKING: bestanden die zonder problemen zijn versnipperd of schoongemaakt, worden niet in de logboekbestanden vermeld.

Er wordt één logboekbestand gemaakt voor shredbewerkingen en een ander voor schoonmaakbewerkingen. Beide logboekbestanden bevinden zich op de vaste schijf op:

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

11 Device Access Manager for HP ProtectTools (alleen bepaalde modellen)

Beheerders van het besturingssysteem Windows® gebruiken Device Access Manager for HP ProtectTools om de toegang tot de apparaten op een systeem te regelen en om het systeem te beschermen tegen ongeoorloofde toegang:

- Voor iedere gebruiker worden apparaatprofielen gemaakt om te definiëren tot welke apparaten zij toegang hebben.
- Gebruikers kunnen ook in groepen worden ingedeeld, zoals in de vooraf gedefinieerde groep Device Administrators, of in door de gebruiker gedefinieerde groepen in het onderdeel Computerbeheer van Systeembeheer in het Configuratiescherm.
- De toegang tot een apparaat kan worden toegestaan of geweigerd op basis van het lidmaatschap van een groep.
- Voor apparaatklassen als cd-rom-drives en dvd-drives kan de lees- en schrijftoegang afzonderlijk worden toegestaan of geweigerd.

Aan een beperkt aantal gebruikers kan ook toestemming worden gegeven om het toegangsbeleid voor het apparaat te lezen en te wijzigen.

Instelprocedures

Device Access Manager openen

U opent Device Access Manager als volgt:

1. Klik achtereenvolgens op **Start**, **Alle programma's**, **HP** en **HP ProtectTools Administrative Console**.
2. Klik in het linkerdeelvenster op **Device Access Manager**.

Apparaattoegang configureren

Device Access Manager for HP ProtectTools biedt drie verschillende weergaven:

- In de weergave Simple Configuration (Eenvoudige configuratie) wordt voor leden van de groep Device Administrators de toegang tot apparaatklassen toegestaan of geweigerd.
- In de weergave Device Class Configuration (Apparaatklasseconfiguratie) wordt voor specifieke gebruikers of groepen de toegang tot bepaalde typen apparaten of specifieke apparaten toegestaan of geweigerd.
- In de weergave User Access Settings (Instellingen gebruikerstoegang) wordt opgegeven welke gebruikers de gegevens in de Simple Configuration (Eenvoudige configuratie) en de Device Class Configuration (Apparaatklasseconfiguratie) kunnen weergeven of wijzigen.

Groep Device Administrators

Wanneer Device Access Manager wordt geïnstalleerd, wordt een groep Device Administrators gemaakt.

De systeembeheerder kan een eenvoudig apparaattoegangsbeleid implementeren door de toegang tot een reeks apparaatklassen te weigeren, tenzij een gebruiker als "vertrouwd" is aangemerkt (met betrekking tot de apparaattoegang). De handigste manier om onderscheid te maken tussen "vertrouwde apparaatgebruikers" en "niet-vertrouwde apparaatgebruikers" is om alle "vertrouwde apparaatgebruikers" lid te maken van de groep Device Administrators. Door leden van de groep Device Administrators via de weergave Simple Configuration (Eenvoudige configuratie) of Device Class Configuration (Apparaatklasseconfiguratie) toegang tot apparaten te geven, wordt ervoor gezorgd dat de "vertrouwde apparaatgebruikers" volledige toegang hebben tot de opgegeven reeks apparaatklassen.

OPMERKING: wanneer een gebruiker wordt toegevoegd aan de groep Device Administrators, krijgt de gebruiker niet automatisch toegang tot apparaten. In de weergave Simple Configuration (Eenvoudige configuratie) kan echter aan "vertrouwde apparaatgebruikers" toegang tot de benodigde reeks apparaatklassen worden verleend.

U voegt als volgt gebruikers toe aan de groep Device Administrators:

- Gebruik voor Windows 7, Vista of XP Professional de standaard-MMC-module "Lokale gebruikers en groepen".
- Typ voor Home-versies van Windows 7, Vista® of XP de volgende tekst in het opdrachtpromptvenster, terwijl u bent aangemeld bij een account met voldoende rechten:

```
c:\> net localgroup "Device Administrators" gebruikersnaam /ADD
```

Eenvoudige configuratie

Beheerders en geautoriseerde gebruikers kunnen in de weergave Simple Configuration (Eenvoudige configuratie) de toegang tot de volgende apparaatklassen wijzigen voor alle gebruikers die geen Device Administrators zijn:

OPMERKING: om in deze weergave gegevens over de apparaattoegang te kunnen lezen, moet in de weergave **User Access Settings** (Instellingen gebruikerstoegang) leestoegang aan de gebruiker of groep zijn verleend. Om in deze weergave gegevens over de apparaattoegang te kunnen wijzigen, moet in de weergave **User Access Settings** (Instellingen gebruikerstoegang) wijzigtoegang aan de gebruiker of groep zijn verleend.

- Alle verwisselbare media (diskettes, USB-flashdrives, enzovoorts)
- Alle dvd/cd-rom-drives
- Alle seriële en parallelle poorten
- Alle Bluetooth®-apparaten
- Alle infraroodapparaten
- Alle modemapparaten
- Alle PCMCIA-apparaten
- Alle 1394-apparaten

U kunt als volgt de toegang tot een apparaatklasse toestaan of weigeren voor alle gebruikers die geen Device Administrators zijn:

1. Klik in het linkerdeelvenster van **HP ProtectTools Administrative Console** op **Device Access Manager** en klik vervolgens op **Simple Configuration** (Eenvoudige configuratie).
2. Schakel in het rechterdeelvenster het selectievakje voor een apparaatklasse of een specifiek apparaat in om de toegang te weigeren. Schakel het selectievakje uit om de toegang tot die apparaatklasse of het specifieke apparaat toe te staan.

   Als een selectievakje lichter gekleurd is, zijn de waarden die op het toegangsscenario van invloed zijn, gewijzigd vanuit de weergave Device Class Configuration (Apparaatklasseconfiguratie). Als u de waarden wilt terugzetten op de eenvoudige instellingen, klikt u op het selectievakje om het uit of in te schakelen en klikt u vervolgens op **Yes** (Ja) om de instellingen te bevestigen.
3. Klik op **Save** (Opslaan).

   OPMERKING: als de achtergrondservice niet actief is, wordt een dialoogvenster geopend met de vraag of u de service wilt starten. Klik op **Yes** (Ja).
4. Klik op **OK**.

Achtergrondservice starten

Voordat apparaatprofielen kunnen worden toegepast, wordt een dialoogvenster geopend waarin u wordt gevraagd of u de achtergrondservice HP ProtectTools Device Locking/Auditing wilt starten. Klik op **Yes** (Ja). De achtergrondservice wordt gestart en wordt daarna automatisch gestart wanneer het systeem wordt opgestart.

OPMERKING: de vraag met betrekking tot de achtergrondservice wordt alleen weergegeven als er een apparaatprofiel is gedefinieerd.

Beheerders kunnen deze service ook starten of stoppen:

1. Klik op **Start** en vervolgens op **Configuratiescherm**.
2. Klik op **Systeembeheer** en klik vervolgens op **Services**.
3. Zoek de service **HP ProtectTools Device Locking/Auditing**.

Wanneer de service Device Locking/Auditing wordt gestopt, wordt de apparaatvergrendeling niet gestopt. Er zijn twee elementen die van invloed zijn op apparaatvergrendeling:

- Service Device Locking/Auditing
- Stuurprogramma DAMDrv.sys

Wanneer de service wordt gestart, wordt het apparaatstuurprogramma gestart, maar wanneer de service wordt gestopt, wordt het stuurprogramma niet gestopt.

Als u wilt vaststellen of de achtergrondservice actief is, opent u een opdrachtpromptvenster en typt u sc query flcdlock.

Als u wilt vaststellen of het apparaatstuurprogramma actief is, opent u een opdrachtpromptvenster en typt u sc query damdrv.

Apparaatklasseconfiguratie

De lijsten met gebruikers en groepen waaraan wel of geen toegangsrechten voor apparaatklassen of specifieke apparaten zijn verleend, kunnen worden weergegeven en gewijzigd door beheerders en geautoriseerde gebruikers.

OPMERKING: om in deze weergave gegevens over de apparaattoegang te kunnen lezen, moet in de weergave **User Access Settings** (Instellingen gebruikerstoegang) leestoegang aan de gebruiker of groep zijn verleend. Om in deze weergave gegevens over de apparaattoegang te kunnen wijzigen, moet in de weergave **User Access Settings** (Instellingen gebruikerstoegang) wijzigtoegang aan de gebruiker of groep zijn verleend.

De weergave Device Class Configuration (Apparaatklasseconfiguratie) bestaat uit de volgende gedeelten:

- **Device List** (Lijst met apparaten): hier worden alle apparaatklassen en apparaten weergegeven die nu in het systeem zijn geïnstalleerd of die eerder op het systeem waren geïnstalleerd.
  - De beveiliging wordt doorgaans toegepast op een apparaatklasse. De geselecteerde gebruiker of groep heeft toegang tot elk apparaat in de apparaatklasse.
  - De beveiliging kan ook per apparaat worden ingesteld.
- **User List** (Lijst met gebruikers): hier worden alle gebruikers en groepen weergegeven die wel of geen toegang hebben tot de geselecteerde apparaatklasse of het specifieke apparaat.
  - De vermelding in de lijst met gebruikers kan gelden voor een specifieke gebruiker of voor een groep waarvan de gebruiker lid is.
  - Als de vermelding van een gebruiker of groep niet beschikbaar is in de lijst met gebruikers, is de instelling overgenomen uit de apparaatklasse in de Device List (Lijst met apparaten) of uit de map Class (Klasse).
  - Voor sommige apparaatklassen, zoals dvd's en cd-rom's, kan de toegang verder worden geregeld door afzonderlijk toegang voor lees- en schrijfbewerkingen te verlenen of te weigeren.

    Net als voor andere apparaten en klassen, kunnen de lees- en schrijfrechten worden overgenomen. Zo kan bijvoorbeeld de leestoegang zijn overgenomen van een hogere klasse, terwijl voor een bepaalde gebruiker of groep de schrijftoegang specifiek is geweigerd.

    OPMERKING: als het selectievakje Read (Lezen) leeg is, heeft de toegangsvermelding geen effect op de leestoegang tot het apparaat. De leestoegang tot het apparaat wordt noch verleend, noch geweigerd.

    Voorbeeld 1: Als aan een gebruiker of groep geen schrijftoegang tot een apparaat of apparaatklasse is verleend:

    Aan dezelfde gebruiker, dezelfde groep of een lid van dezelfde groep kan alleen voor een apparaat onder dit apparaat in de apparatenhiërarchie schrijftoegang of lees- en schrijftoegang worden verleend.

    Voorbeeld 2: Als aan een gebruiker of groep schrijftoegang tot een apparaat of apparaatklasse is verleend:

    Aan dezelfde gebruiker, dezelfde groep of een lid van dezelfde groep kan alleen voor hetzelfde apparaat of een apparaat onder dit apparaat in de apparatenhiërarchie de schrijftoegang of lees- en schrijftoegang worden geweigerd.

    Voorbeeld 3: Als aan een gebruiker of groep leestoegang tot een apparaat of apparaatklasse is verleend:

    Aan dezelfde gebruiker, dezelfde groep of een lid van dezelfde groep kan alleen voor hetzelfde apparaat of een apparaat onder dit apparaat in de apparatenhiërarchie de leestoegang of lees- en schrijftoegang worden geweigerd.

    Voorbeeld 4: Als aan een gebruiker of groep geen leestoegang tot een apparaat of apparaatklasse is verleend:

Aan dezelfde gebruiker, dezelfde groep of een lid van dezelfde groep kan alleen voor een apparaat onder dit apparaat in de apparatenhiërarchie leestoegang of lees- en schrijftoegang worden verleend.

Voorbeeld 5: Als aan een gebruiker of groep lees- en schrijftoegang tot een apparaat of apparaatklasse is verleend:

Aan dezelfde gebruiker, dezelfde groep of een lid van dezelfde groep kan alleen voor hetzelfde apparaat of een apparaat onder dit apparaat in de apparatenhiërarchie de schrijftoegang of lees- en schrijftoegang worden geweigerd.

Voorbeeld 6: Als aan een gebruiker of groep geen lees- en schrijftoegang tot een apparaat of apparaatklasse is verleend:

Aan dezelfde gebruiker, dezelfde groep of een lid van dezelfde groep kan alleen voor een apparaat onder dit apparaat in de apparatenhiërarchie leestoegang of lees- en schrijftoegang worden verleend.

Toegang weigeren aan een gebruiker of groep

U kunt als volgt een gebruiker of groep de toegang tot een apparaat of een apparaatklasse weigeren:

1. Klik in het linkerdeelvenster van **HP ProtectTools Administrative Console** op **Device Access Manager** en klik vervolgens op **Device Class Configuration** (Apparaatklasseconfiguratie).
2. Klik in de apparatenlijst op de apparaatklasse die u wilt configureren.
   - Apparaatklasse
   - Alle apparaten
   - Afzonderlijk apparaat
3. Klik onder **User/Groups** (Gebruiker/groepen) op de gebruiker of groep waaraan u de toegang wilt weigeren.
4. Klik op **Deny** (Weigeren) naast een gebruiker of groep.
5. Klik op **Save** (Opslaan).

OPMERKING: wanneer op hetzelfde apparaatniveau toegangsrechten zijn verleend of geweigerd voor een gebruiker, telt toegangsweigering zwaarder dan toegangsverlening.

Toegang toestaan aan een gebruiker of groep

U kunt als volgt een gebruiker of groep toestemming geven om toegang tot een apparaat of apparaatklasse te krijgen:

1. Klik in het linkerdeelvenster van **HP ProtectTools Administrative Console** op **Device Access Manager** en klik vervolgens op **Device Class Configuration** (Apparaatklasseconfiguratie).
2. Klik in de apparatenlijst op een van de volgende:
   - Apparaatklasse
   - Alle apparaten
   - Afzonderlijk apparaat
3. Klik op **Add** (Toevoegen).

Het dialoogvenster **Select Users or Groups** (Gebruikers of groepen selecteren) wordt geopend.

4. Klik op **Advanced** (Geavanceerd) en klik vervolgens op **Find Now** (Nu zoeken) om te zoeken naar de gebruikers of groepen die u wilt toevoegen.
5. Klik op een gebruiker of een groep die u wilt toevoegen aan de lijst met beschikbare gebruikers en groepen en klik vervolgens op **OK**.
6. Klik nogmaals op **OK**.
7. Klik op **Allow** (Toestaan) om deze gebruiker of groep toegang te verlenen.
8. Klik op **Save** (Opslaan).

Toegang voor een gebruiker of groep verwijderen

U kunt als volgt voor een gebruiker of een groep de toestemming om toegang tot een apparaat of apparaatklasse te krijgen intrekken:

1. Klik in het linkerdeelvenster van **HP ProtectTools Administrative Console** op **Device Access Manager** en klik vervolgens op **Device Class Configuration** (Apparaatklasseconfiguratie).
2. Klik in de apparatenlijst op de apparaatklasse die u wilt configureren.
   - Apparaatklasse
   - Alle apparaten
   - Afzonderlijk apparaat
3. Klik onder **User/Groups** (Gebruiker/groepen) op de gebruiker of groep die u wilt verwijderen en klik vervolgens op **Remove** (Verwijderen).
4. Klik op **Save** (Opslaan).

Toegang tot een apparaatklasse verlenen aan één gebruiker van een groep

U kunt als volgt één gebruiker toegang geven tot een apparaatklasse, terwijl u alle anderen in die gebruikersgroep de toegang tot die apparaatklasse ontzegt:

1. Klik in het linkerdeelvenster van **HP ProtectTools Administrative Console** op **Device Access Manager** en klik vervolgens op **Device Class Configuration** (Apparaatklasseconfiguratie).
2. Klik in de apparatenlijst op de apparaatklasse die u wilt configureren.
   - Apparaatklasse
   - Alle apparaten
   - Afzonderlijk apparaat
3. Selecteer onder **User/Groups** (Gebruiker/groepen) de groep waaraan u de toegang wilt ontzeggen en klik vervolgens op**Deny** (Weigeren).
4. Navigeer naar de map onder die van de gewenste klasse en voeg vervolgens de specifieke gebruiker toe.
5. Klik op **Allow** (Toestaan) om deze gebruiker toegang te verlenen.
6. Klik op **Save** (Opslaan).

Toegang tot een specifiek apparaat verlenen aan één gebruiker van een groep

Beheerders kunnen een gebruiker toegang tot een specifiek apparaat verlenen, terwijl alle anderen in die gebruikersgroep de toegang tot alle apparatuur in die klasse wordt ontzegd:

1. Klik in het linkerdeelvenster van **HP ProtectTools Administrative Console** op **Device Access Manager** en klik vervolgens op **Device Class Configuration** (Apparaatklasseconfiguratie).
2. Klik in de apparatenlijst op de apparaatklasse die u wilt configureren en navigeer vervolgens naar de map onder deze klasse.
3. Klik op **Add** (Toevoegen). Het dialoogvenster **Select Users or Groups** (Gebruikers of groepen selecteren) wordt geopend.
4. Klik op **Advanced** (Geavanceerd) en klik vervolgens op **Find Now** (Nu zoeken) om te zoeken naar de groep van de gebruiker waaraan u de toegang tot alle apparaten in de klasse wilt ontzeggen.
5. Klik op de groep en klik vervolgens op **OK**.
6. Navigeer naar het specifieke apparaat onder de apparaatklasse waartoe u de gebruiker toegang wilt verlenen.
7. Klik op **Add** (Toevoegen). Het dialoogvenster **Select Users or Groups** (Gebruikers of groepen selecteren) wordt geopend.
8. Klik op **Advanced** (Geavanceerd) en klik vervolgens op **Find Now** (Nu zoeken) om te zoeken naar de gebruikers of groepen die u wilt toevoegen.
9. Klik op de gebruiker die u toegang wilt verlenen en klik vervolgens op **OK**.
10. Klik op **Allow** (Toestaan) om deze gebruiker toegang te verlenen.
11. Klik op **Save** (Opslaan).

Configuratie herstellen

△ **VOORZICHTIG:** wanneer u de configuratie herstelt, worden alle wijzigingen in de configuratie van het apparaat genegeerd en worden alle instellingen teruggezet op de fabriekswaarden.

U zet als volgt de configuratie-instellingen terug op de fabriekswaarden:

1. Klik in het linkerdeelvenster van **HP ProtectTools Administrative Console** op **Device Access Manager** en klik vervolgens op **Device Class Configuration** (Apparaatklasseconfiguratie).
2. Klik op de knop **Reset** (Opnieuw instellen).
3. Klik op **Yes** (Ja) om uw keuze te bevestigen.
4. Klik op **Save** (Opslaan).

Geavanceerde taken

Toegang tot de configuratie-instellingen regelen

In de weergave **User Access Settings** (Instellingen gebruikerstoegang) geven beheerders op welke groepen of gebruikers de pagina's Simple Configuration (Eenvoudige configuratie) en Device Class Configuration (Apparaatklasseconfiguratie) mogen gebruiken.

OPMERKING: een gebruiker of groep moet "Full User Administrator Rights" (Volledige gebruikersbeheerdersrechten) hebben om de instellingen in de weergave User Access Settings (Instellingen gebruikerstoegang) te kunnen wijzigen.

- Aan een gebruiker of groep moet het toegangsrecht "View (Read-only) Configuration Settings" (Configuratie-instellingen weergeven (alleen-lezen)) zijn verleend in de weergave User Access Settings (Instellingen gebruikerstoegang) om de gegevens van de Simple Configuration (Eenvoudige configuratie) en Device Class Configuration (Apparaatklasseconfiguratie) te kunnen bekijken.
- Aan een gebruiker of groep moet het toegangsrecht "Change Configuration Settings" (Configuratie-instellingen wijzigen) zijn verleend in de weergave User Access Settings (Instellingen gebruikerstoegang) om de gegevens van de Simple Configuration (Eenvoudige configuratie) en Device Class Configuration (Apparaatklasseconfiguratie) te kunnen wijzigen.

OPMERKING: zelfs aan de leden van de groep Administrators moet leestoegang worden verleend, willen zij de weergaven Simple Configuration (Eenvoudige configuratie) en Device Class Configuration (Apparaatklasseconfiguratie) kunnen zien. Bovendien moet aan hen wijzigtoegang zijn verleend om gegevens te kunnen wijzigen in de weergaven Simple Configuration (Eenvoudige configuratie) en Device Class Configuration (Apparaatklasseconfiguratie).

OPMERKING: nadat de toegangsniveaus voor alle gebruikers en groepen zijn geëvalueerd, krijgt een gebruiker geen toegang tot een bepaald niveau als voor deze gebruiker Allow (Toestaan) of Deny (Weigeren) voor dat toegangsniveau is geselecteerd.

Toegang geven aan een bestaande groep of gebruiker

U kunt een bestaande groep of gebruiker als volgt toestemming geven om de configuratie-instellingen weer te geven of te wijzigen:

1. Klik in het linkerdeelvenster van **HP ProtectTools Administrative Console** op **Device Access Manager** en klik vervolgens op **User Access Settings** (Instellingen gebruikerstoegang).
2. Klik op de groep of gebruiker waaraan u toegang wilt geven.
3. Klik onder **Permissions** (Machtigingen) op **Allow** (Toestaan) voor elk type machtiging dat u de geselecteerde groep of gebruiker wilt verlenen:

OPMERKING: de machtigingen worden cumulatief verleend. Een gebruiker waaraan bijvoorbeeld het recht "Change Configuration Settings (Configuratie-instellingen wijzigen)" is verleend, krijgt automatisch de machtiging "View (Read-only) Configuration Settings" (Configuratie-instellingen weergeven (alleen-lezen)). Een gebruiker waaraan "Full User Administrator Rights" (Volledige gebruikersbeheerdersrechten) zijn verleend, krijgt ook de machtigingen "Change Configuration Settings" (Configuratie-instellingen wijzigen) en "View (Read-only) Configuration Settings" (Configuratie-instellingen weergeven (alleen-lezen)).

- Full User Administrator Rights (Volledige gebruikersbeheerdersrechten)
- Change Configuration Settings (Configuratie-instellingen wijzigen)
- View (Read-only) Configuration Settings (Configuratie-instellingen weergeven (alleen-lezen))

4. Klik op **Save** (Opslaan).

Toegang weigeren aan een bestaande groep of gebruiker

U kunt als volgt aan een bestaande groep of gebruiker toestemming weigeren om de configuratie-instellingen weer te geven of te wijzigen:

1. Klik in het linkerdeelvenster van **HP ProtectTools Administrative Console** op **Device Access Manager** en klik vervolgens op **User Access Settings** (Instellingen gebruikerstoegang).
2. Klik op de groep of gebruiker waaraan u de toegang wilt ontzeggen.
3. Klik onder **Permissions** (Machtigingen) op **Deny** (Weigeren) voor elk type machtiging dat u de geselecteerde groep of gebruiker wilt ontzeggen:
   - Full User Administrator Rights (Volledige gebruikersbeheerdersrechten)
   - Change Configuration Settings (Configuratie-instellingen wijzigen)
   - View (Read-only) Configuration Settings (Configuratie-instellingen weergeven (alleen-lezen))
4. Klik op **Save** (Opslaan).

Nieuwe groep of gebruiker toevoegen

U kunt een nieuwe groep of gebruiker als volgt toestemming geven om de configuratie-instellingen weer te geven of te wijzigen:

1. Klik in het linkerdeelvenster van **HP ProtectTools Administrative Console** op **Device Access Manager** en klik vervolgens op **User Access Settings** (Instellingen gebruikerstoegang).
2. Klik op **Add** (Toevoegen). Het dialoogvenster **Select Users or Groups** (Gebruikers of groepen selecteren) wordt geopend.
3. Klik op **Advanced** (Geavanceerd) en klik vervolgens op **Find Now** (Nu zoeken) om te zoeken naar de gebruikers of groepen die u wilt toevoegen.
4. Klik op een groep of gebruiker, klik op **OK** en klik vervolgens nogmaals op **OK**.
5. Klik op **Allow** (Toestaan) om deze gebruiker toegang te verlenen.
6. Klik op **Save** (Opslaan).

Toegang voor groep of gebruiker verwijderen

U kunt de toestemming voor een groep of gebruiker om de configuratie-instellingen weer te geven of te wijzigen, als volgt verwijderen:

1. Klik in het linkerdeelvenster van **HP ProtectTools Administrative Console** op **Device Access Manager** en klik vervolgens op **User Access Settings** (Instellingen gebruikerstoegang).
2. Klik op een groep of gebruiker en klik op **Remove** (Verwijderen).
3. Klik op **Save** (Opslaan).

Gerelateerde documentatie

Device Access Manager for HP ProtectTools is compatibel met HP ProtectTools Enterprise Device Access Manager, de versie voor de grootzakelijke markt. Wanneer u met de Enterprise versie werkt, geeft Device Access Manager for HP ProtectTools alleen-lezentoegang tot de voorzieningen van het product.

Meer informatie over Device Access Manager for HP ProtectTools is te vinden op http://www.hp.com/hps/security/products.

12 LoJack Pro voor HP ProtectTools

Met de Computrace-productlijn van Absolute Software kunnen gebruikers hun HP computers traceren en de gegevensbeveiliging ervan verbeteren. De Computrace LoJack-producten kunnen ook bijdragen aan vermindering van het aantal computers dat kwijtraakt en aan het opsporen van gestolen computers.

Ga als volgt te werk om het Computrace-product te activeren:

1. Klik achtereenvolgens op **Start**, **Alle programma's** en **HP ProtectTools Security Manager**.
2. Klik op **Theft Recovery** (Opsporen bij diefstal) en klik op **Activate Now** (Nu activeren).

   In de standaardwebbrowser wordt een aanmeldingswebsite geopend. Hier kunt u een van de drie Computrace-producten selecteren en kopen die beschikbaar zijn voor HP ProtectTools:

   - **Computrace Data Delete**: gegevens op afstand verwijderen, apparaat "bevriezen" en basisvoorzieningen voor opsporing en rapportage van computerproducten.
   - **Computrace LoJack Pro**: gegevens op afstand verwijderen, apparaat "bevriezen", basisvoorzieningen voor opsporing en rapportage van computerproducten en beheer van opsporing bij diefstal.
   - **Computrace LoJack Pro Premium**: gegevens op afstand verwijderen, apparaat "bevriezen", geavanceerde voorzieningen voor opsporing en rapportage van computerproducten, geolocatie en geofencing, en beheer van opsporing bij diefstal.

De Computrace Agent is geïntegreerd in het BIOS of HP zakelijke notebookcomputers. De Agent is bij aflevering van de computer uitgeschakeld. Nadat u een abonnement heeft genomen, kan de Agent worden geactiveerd. Met de geïntegreerde Agent kan het besturingssysteem opnieuw worden geïnstalleerd en kunnen vaste schijven opnieuw worden geformatteerd.

OPMERKING: Er zijn abonnementsperiodes van één tot vijf jaar mogelijk. Raadpleeg de abonnementsovereenkomst van Absolute Software voor bijzonderheden. De opsporingsvoorziening is afhankelijk van uw geografische locatie. GPS-tracering wordt alleen op bepaalde modellen met de WWAN-optie ondersteund.

13 Problemen oplossen

HP ProtectTools Security Manager

Korte beschrijving	Gegevens	Oplossing
SmartCards en USB-tokens zijn niet beschikbaar in Security Manager als ze zijn geïnstalleerd nadat Security Manager is geïnstalleerd.	Om smart cards of USB-tokens te kunnen gebruiken in Security Manager, moet de ondersteunende software (stuurprogramma's, PKCS#11-providers, enz.) worden geïnstalleerd voordat Security Manager wordt geïnstalleerd. Als Security Manager al is geïnstalleerd, voert u de volgende stappen uit nadat u de ondersteunende software voor de smartcard of het token heeft geïnstalleerd:	Meld u aan bij Password Manager. Klik in HP ProtectTools Security Manager op **Password Manager**, klik op **Credentials** (Referenties) en klik vervolgens op **Smart Card** (Smartcard) Start de computer opnieuw op als daarom wordt gevraagd.
Sommige applicatiewebpagina's veroorzaken fouten waardoor gebruikers taken niet kunnen uitvoeren of voltooien.	Sommige webapplicaties functioneren niet meer en geven foutmeldingen doordat zij worden geblokkeerd door het functionaliteitenpatroon van Single Sign On. In Internet Explorer wordt bijvoorbeeld **!** weergegeven in een gele driehoek om aan te geven dat een fout is opgetreden.	De voorziening Single Sign On (Single sign-on) van Security Manager ondersteunt niet alle softwarematige webinterfaces. Schakel voor de webpagina in kwestie ondersteuning voor Single Sign On (Single sign-on) uit. Raadpleeg de uitvoerige documentatie met betrekking tot Single Sign On (Single sign-on) in de helpbestanden van de Security Manager software. Als u een specifieke Single Sign On niet kunt uitschakelen voor een bepaalde applicatie, neemt u telefonisch contact op met de technische ondersteuning van HP en vraagt u uw contactpersoon bij de HP klantenservice om ondersteuning van het derde niveau.
De optie **Browse for Virtual Token** (Naar virtueel token bladeren) wordt niet weergegeven gedurende het aanmeldproces.	De gebruiker kan de locatie van een geregistreerd virtueel token in Password Manager niet wijzigen, omdat de bladermogelijkheid is verwijderd om de beveiligingsrisico's te beperken.	De bladeroptie is verwijderd, omdat niet-gebruikers bestanden konden verwijderen, bestanden een nieuwe naam konden geven en Windows konden overnemen.
Domeinbeheerders kunnen Windows-wachtwoorden niet wijzigen. Zelfs niet als ze daartoe geautoriseerd zijn.	Dit gebeurt nadat een domeinbeheerder zich bij een domein heeft aangemeld en met Password Manager de domeinidentiteit registreert via een account met beheerdersrechten op het domein en de lokale pc. Wanneer de domeinbeheerder vanuit Password Manager probeert het Windows-wachtwoord te wijzigen, krijgt de beheerder een aanmeldingsfout: **User**	Het is niet mogelijk om het accountwachtwoord van een domeingebruiker te wijzigen via de optie **Change Windows password** (Windows-wachtwoord wijzigen) in Password Manager. Met Security Manager kunnen alleen de accountwachtwoorden op de lokale pc worden gewijzigd. De domeingebruiker kan zijn/haar wachtwoord wijzigen via de optie **Wachtwoord wijzigen** van **Windows-beveiliging**, maar omdat de domeingebruiker geen fysieke account op de lokale pc heeft, kan in Password Manager alleen het wachtwoord

Korte beschrijving	Gegevens	Oplossing
	account restriction (Beperking gebruikersaccount).	worden gewijzigd dat voor de aanmelding wordt gebruikt.
Er zijn compatibiliteitsproblemen tussen Password Manager en de wachtwoord-GINA van Corel WordPerfect 12.	Als de gebruiker zich aanmeldt bij Password Manager, een document in WordPerfect maakt en het opslaat met wachtwoordbeveiliging, wordt de wachtwoord-GINA niet gedetecteerd of herkend (noch handmatig, noch automatisch).	HP onderzoekt mogelijkheden waarmee dit probleem bij toekomstige productverbeteringen opgelost kan worden.
De knop **Connect** (Verbinding maken) op het scherm wordt niet herkend door Password Manager.	Als de Single Sign On referenties voor Remote Desktop Connection (RDP) zijn ingesteld op **Connect** (Verbinden) wanneer Single Sign On opnieuw wordt gestart, wordt altijd **Save As** (Opslaan als) ingevoerd in plaats van **Connect** (Verbinden).	HP onderzoekt mogelijkheden waarmee dit probleem bij toekomstige productverbeteringen opgelost kan worden.
De gebruiker kan zich niet aanmelden bij Password Manager nadat de standbystand is overgegaan in de hibernationstand (alleen bij Windows XP Service Pack 1).	Nadat op het systeem de hibernationstand en de slaapstand zijn geactiveerd, kan de beheerder of gebruiker zich niet bij Password Manager aanmelden en blijft het Windows-aanmeldscherm staan, ongeacht welke aanmeldreferentie (wachtwoord, vingerafdruk of Java Card) wordt geselecteerd.	Voer een update van Windows naar Service Pack 2 uit via Windows Update. Raadpleeg artikel 813301 van de Microsoft Knowledge Base op http://www.microsoft.com voor meer informatie over de oorzaak van het probleem. De gebruiker moet Password Manager selecteren en zich aanmelden. Nadat de gebruiker zich heeft aangemeld bij Password Manager, wordt de gebruiker gevraagd om zich aan te melden bij Windows (mogelijk moet de gebruiker de Windows-aanmeldoptie selecteren) om het aanmeldproces te voltooien. Als de gebruiker zich eerst bij Windows aanmeldt, moet hij/zij zich handmatig aanmelden bij Password Manager.
Tijdens het beveiligingsproces **Restore Identity** (Identiteit herstellen) gaat de associatie met een virtueel token verloren.	Wanneer een gebruiker zijn identiteit herstelt, kan in Password Manager de koppeling met de locatie van het virtuele token in het aanmeldscherm verloren gaan. Hoewel Password Manager het virtuele token heeft geregistreerd, moet de gebruiker het token opnieuw registreren om de koppeling te herstellen.	Momenteel is dit zo ontworpen. Wanneer Security Manager wordt verwijderd zonder dat de identiteiten worden behouden, wordt het systeemgedeelte (servergedeelte) van het token vernietigd, zodat het token niet meer voor de aanmelding kan worden gebruikt, zelfs als het clientgedeelte van het token wordt hersteld met de optie voor identiteitsherstel. HP onderzoekt momenteel een lange-termijnoplossing.

Device Access Manager for HP ProtectTools

Binnen Device Access Manager is gebruikers de toegang tot apparaten ontzegd, maar de apparaten zijn nog steeds toegankelijk.

- **Toelichting**: De weergaven Simple Configuration (Eenvoudige configuratie) en/of Device Class Configuration (Apparaatklasseconfiguratie) van Device Access Manager zijn gebruikt om de gebruikers de toegang tot de apparaten te ontzeggen. Ondanks dat hun de toegang is geweigerd, hebben gebruikers nog steeds toegang tot de apparaten.
- **Oplossing:**
  - Controleer of de service HP ProtectTools Device Locking is gestart.
  - Klik als beheerder op **Configuratiescherm** en klik vervolgens op **Systeem en onderhoud**. Klik in het venster Systeembeheer op **Services** en zoek de service **HP ProtectTools Device Locking/Auditing**. Controleer of de service is gestart en of het opstarttype **Automatisch** is.

Een gebruiker heeft onverwachts wel of geen toegang tot een apparaat.

- **Toelichting**: Device Access Manager is gebruikt om gebruikers de toegang tot bepaalde apparaten te weigeren en tot andere apparaten toe te staan. Wanneer de gebruikers het systeem gebruiken, hebben zij toegang tot apparaten waartoe zij dachten geen toegang te hebben en hebben zij geen toegang tot apparaten waartoe zij wel dachten toegang te hebben gekregen.
- **Oplossing:**
  - Gebruik Device Class Configuration (Apparaatklasseconfiguratie) in Device Access Manager om de apparaatinstellingen voor de gebruikers te onderzoeken.
  - Klik op **Security Manager**, klik op **Device Access Manager** en klik vervolgens op **Device Class Configuration** (Apparaatklasseconfiguratie). Vouw de niveaus in de structuur met apparaatklassen uit en bekijk de instellingen die voor deze gebruiker gelden. Controleer op eventuele geweigerde machtigingen die zijn ingesteld voor de gebruiker of een Windows-groep waarvan zij lid zijn (zoals Gebruikers of Administrators).

Wat heeft voorrang? Toestaan of Weigeren?

- **Toelichting**: in Device Class Configuration (Apparaatklasseconfiguratie) is de volgende configuratie ingesteld:
  - De machtiging Allow (Toestaan) is verleend aan een Windows-groep (bijvoorbeeld BUILTIN \Administrators), terwijl op hetzelfde niveau in de hiërarchie van apparaatklassen (bijvoorbeeld Dvd-/cd-rom-stations) de machtiging Deny (Weigeren) is verleend aan een andere Windows-groep (bijvoorbeeld BUILTIN\Gebruikers).
  - Welke instelling heeft voorrang als een gebruiker lid is van beide groepen (bijvoorbeeld een beheerder)?
- **Oplossing:**
  - De gebruiker krijgt geen toegang tot het apparaat. Deny (Weigeren) heeft voorrang op Allow (Toestaan).
  - De toegang wordt geweigerd op grond van de manier waarop in Windows de feitelijke machtigingen voor het apparaat worden vastgesteld. Eén groep krijgt geen toegang, terwijl een andere groep wel toegang krijgt, maar de gebruiker is lid van beide groepen. De gebruiker krijgt geen toegang, omdat toegangsweigering zwaarder telt dan toegangsverlening.

- Eén oplossing is om de groep Gebruikers op het niveau van Dvd-/cd-rom-stations de toegang te weigeren en de groep Administrators op het niveau onder Dvd-/cd-rom-stations toegang te geven.
- Een andere oplossing is om specifieke Windows-groepen te maken: één waarbij toegang tot dvd's/cd's wordt toegestaan, en een andere waarvoor de toegang tot dvd's/cd's wordt geweigerd. Vervolgens worden specifieke gebruikers toegevoegd aan de van toepassing zijnde groep.

In de Simple Configuration (Eenvoudige configuratie) is een apparaattoegangsbeleid gedefinieerd, maar beheerders hebben geen toegang tot apparaten.

- **Toelichting**: In de weergave Simple Configuration (Eenvoudige configuratie) wordt de toegang aan Gebruikers en Gasten geweigerd en aan Device Administrators toegestaan.
- **Oplossing:** Voeg de beheerder toe aan de groep Device Administrators.

Overige problemen

Invloed op software — korte beschrijving	Meer informatie	Oplossing
Security Manager — waarschuwing ontvangen: **The security application can not be installed until the HP Protect Tools Security Manager is installed** (De beveiligingsapplicatie kan niet worden geïnstalleerd voordat HP ProtectTool Security Manager is geïnstalleerd).	Alle beveiligingsapplicaties, zoals Java Card Security en biometrische lezers, zijn uitbreidbare plug-ins voor de interface van Security Manager. Security Manager moet zijn geïnstalleerd voordat een door HP goedgekeurde beveiligingsplug-in kan worden geladen.	De Security Manager software moet zijn geïnstalleerd voordat u een beveiligingsinvoegtoepassing installeert.
HP ProtectTools Security Manager: soms wordt bij het afsluiten van de Security Manager interface een foutbericht weergegeven.	Af en toe (1 op de 12 gebeurtenissen), wordt een foutbericht weergegeven wanneer u op de knop Sluiten in de rechterbovenhoek van het scherm klikt om Security Manager af te sluiten voordat alle invoegtoepassingen volledig zijn geladen.	Dat komt door timing-afhankelijkheid van de laadtijd van invoegtoepassingen bij het afsluiten en opnieuw starten van Security Manager. Aangezien PTHOST.exe de shell is waarin de andere applicaties (invoegtoepassingen) worden uitgevoerd, is het afhankelijk van de invoegtoepassing of de laadtijd wordt voltooid (services). Deze fout wordt gegenereerd wanneer u de shell sluit voordat de invoegtoepassing volledig is geladen. Wacht tot in Security Manager het bericht Services loading (Services worden geladen) niet langer bovenin het Security Manager venster wordt weergegeven en alle invoegtoepassingen in de linkerkolom worden weergegeven. Geef de invoegtoepassingen genoeg tijd om te laden, om fouten te voorkomen.
HP ProtectTools: onbeperkte toegang of onbeperkte beheerdersrechten vormen een beveiligingsrisico.	Als de clientcomputer onbeperkt toegankelijk is, loopt u een aanzienlijk beveiligingsrisico op onder andere de volgende gebieden: • PSD wissen • Kwaadwillige wijzigingen in gebruikersinstellingen • Beveiligingsbeleid en -functies uitschakelen	Beheerders wordt aangeraden "optimale werkwijzen" toe te passen bij het beperken van de bevoegdheden van eindgebruikers en het beperken van gebruikerstoegang. Aan onbevoegde gebruikers moeten geen beheerdersbevoegdheden worden toegekend.

Woordenlijst

aanmelding Een object binnen Security Manager dat bestaat uit een gebruikersnaam en een wachtwoord (en eventueel andere geselecteerde gegevens) aan de hand waarvan een gebruiker zich kan aanmelden bij websites of programma's.

Aanmeldingsbeveiliging van Windows Hiermee worden uw Windows-account(s) beveiligd doordat specifieke referenties nodig zijn om toegang te krijgen.

achtergrondservice De achtergrondservice HP ProtectTools Device Locking/Auditing, die actief moet zijn om een apparaattoegangsbeleid te kunnen toepassen. De service kan worden weergegeven vanuit de toepassing Services in het onderdeel Systeembeheer van het Configuratiescherm. Als de service niet actief is, wordt automatisch geprobeerd de service te starten wanneer een apparaattoegangsbeleid wordt toegepast.

activering De taak die moet worden voltooid voordat de voorzieningen van Drive Encryption toegankelijk zijn. Drive Encryption wordt geactiveerd via de setup-wizard voor HP ProtectTools. Alleen een beheerder kan Drive Encryption activeren. De activeringsprocedure bestaat uit het activeren van de software, het coderen van de schijfeenheid, het maken van een gebruikersaccount en het maken van een back-up van de coderingssleutel op een verwisselbaar opslagapparaat.

apparaatklasse Alle apparaten van een bepaald type, zoals schijfeenheden.

apparaattoegangsbeleid De lijst met apparaten waarvoor aan een gebruiker toegang wordt verleend of geweigerd.

ATM Automatic Technology Manager. Hiermee kunnen netwerkbeheerders systemen op afstand beheren op BIOS-niveau.

automatische versnippering Geplande versnippering (shredbewerking) die de gebruiker instelt in File Sanitizer.

back-up maken Het gebruiken van de back-upvoorziening om een kopie van belangrijke programmagegevens op te slaan op een locatie buiten het programma. De back-up kan later worden gebruikt om de gegevens terug te zetten op dezelfde of een andere computer.

beheerder *Zie* Windows-beheerder.

beveiligde aanmeldingsmethode De methode die wordt gebruikt voor aanmelding bij de computer.

biometrisch Een categorie referenties die voor de identificatie van een gebruiker gebruikmaken van een fysieke eigenschap, zoals een vingerafdruk.

certificeringsinstantie Een organisatie die de certificaten uitgeeft die nodig zijn voor een public key infrastructure.

codering Een cryptografische procedure, zoals het gebruik van een algoritme, die wordt gebruikt om platte tekst om te zetten in vercijferde tekst, zodat niet-gemachtigde ontvangers de gegevens niet kunnen lezen. Er zijn vele

manieren voor het coderen van gegevens, die de basis vormen van netwerkbeveiliging. Veelvoorkomende coderingsmethoden zijn Data Encryption Standard en codering door middel van publieke sleutels.

console Een centrale locatie van waaruit de voorzieningen en instellingen van HP ProtectTools Administrative Console beschikbaar zijn en kunnen worden beheerd.

cryptografie Het coderen en decoderen van gegevens, zodat deze alleen door bepaalde gebruikers kunnen worden gedecodeerd.

CSP (cryptographic service provider) Een leverancier of bibliotheek van cryptografische algoritmen die in een vastgelegde interface kunnen worden gebruikt om bepaalde cryptografische functies uit te voeren.

dashboard Een centrale locatie van waaruit de voorzieningen en instellingen van Security Manager for HP ProtectTools beschikbaar zijn en kunnen worden beheerd.

decodering Een cryptografische procedure voor het omzetten van gecodeerde gegevens naar platte tekst.

digitaal certificaat Elektronische referenties die de identiteit van een individu of een bedrijf bevestigen door de identiteit van de eigenaar van het digitale certificaat te koppelen aan een stel elektronische sleutels die worden gebruikt om digitale informatie te ondertekenen.

digitale handtekening Bij een bestand verzonden gegevens die de afzender van het materiaal verifiëren en die aantonen dat het bestand na ondertekening niet is gewijzigd.

domein Groep computers die deel uitmaken van een netwerk en die een gemeenschappelijke directorydatabase delen. Elk domein heeft een unieke naam en een set gemeenschappelijke regels en procedures.

Drive Encryption Beschermt uw gegevens door de vaste schijf of schijven te coderen, waardoor de gegevens onleesbaar zijn voor degenen die niet de juiste bevoegdheden hebben.

Drive Encryption aanmeldingsscherm Een aanmeldingsscherm dat verschijnt voordat Windows wordt gestart. Gebruikers moeten hun Windows-gebruikersnaam en -wachtwoord opgegeven, of de pincode van een Java Card. In de meeste gevallen zorgt het invoeren van de juiste informatie op het aanmeldingsscherm van Drive Encryption ervoor dat u rechtstreeks toegang tot Windows heeft zonder u opnieuw te hoeven aanmelden op het aanmeldingsscherm van Windows.

DriveLock. Beveiligingsvoorziening die de vaste schijf koppelt aan een gebruiker. De gebruiker moet bij het opstarten van de computer het juiste DriveLock-wachtwoord typen.

eenvoudige verwijdering Verwijdering van de verwijzing in Windows naar een gegevensbestanddeel. De inhoud van het gegevensbestanddeel blijft op de vaste schijf staan tot de inhoud wordt overschreven bij het opschonen van vrije ruimte.

Encryption File System (EFS) Een systeem waarmee alle bestanden en submappen in een geselecteerde map worden gecodeerd.

geautoriseerde gebruiker Een gebruiker die in de weergave User Access Settings (Instellingen gebruikerstoegang) toestemming heeft gekregen om in de weergave Simple Configuration (Eenvoudige configuratie) of Device Class Configuration (Apparaatklasseconfiguratie) de configuratie-instellingen te bekijken of te wijzigen.

gebruiker Iedereen die het inschrijvingsproces van Drive Encryption heeft doorlopen. Gebruikers die geen beheerder zijn, hebben beperkte rechten in Drive Encryption. Ze kunnen zich alleen inschrijven (met toestemming van de beheerder) en aanmelden.

gegevensbestanddeel Een gegevenscomponent bestaande uit persoonlijke informatie of bestanden, historiegegevens, webgerelateerde gegevens, enzovoort, op de vaste schijf.

groep Een groep gebruikers die dezelfde mate van toegang tot een apparaatklasse of een specifiek apparaat hebben.

handmatige versnippering Onmiddellijke versnippering van een of meer geselecteerde gegevensbestanddelen, waarbij het schema voor automatische versnippering wordt genegeerd.

handtekeningregel Een ruimte bestemd voor de visuele weergave van een digitale handtekening. Wanneer een document wordt ondertekend, worden de naam en verificatiemethode van de ondertekenaar weergegeven. Ook de ondertekeningsdatum en de titel van de ondertekenaar kunnen worden opgenomen.

herstart Proces waarbij de computer opnieuw wordt opgestart.

HP SpareKey Backupkopie van coderingssleutel voor een schijfeenheid.

identiteit In de HP ProtectTools Security Manager een verzameling verificatiegegevens en instellingen, die wordt gezien als een account of profiel van een bepaalde gebruiker.

id-kaart Een Windows Sidebar-gadget met uw gebruikersnaam en een door u gekozen afbeelding, die als visueel identificatiemiddel dient. Klik op de id-kaart om HP ProtectTools Administrative Console te openen.

Java Card Een verwisselbare kaart die in de computer wordt geplaatst. De kaart bevat identificatiegegevens voor aanmelding. Als u zich met een Java Card wilt aanmelden op het aanmeldingsscherm van Drive Encryption, moet u de Java Card in de computer plaatsen en uw gebruikersnaam en de pincode van de Java Card typen.

lijst met vertrouwde contactpersonen Een lijst met de vertrouwde contactpersonen.

Live Messenger History Viewer (Live Messenger-geschiedenis) Onderdeel van Privacy Manager Chat waarmee u gecodeerde sessies uit de chathistorie kunt zoeken en weergeven.

migratie Een taak die het beheer, het herstel en het overbrengen van Privacy Manager-certificaten en vertrouwde contactpersonen mogelijk maakt.

netwerkaccount Een gebruikersaccount of beheerdersaccount voor Windows, op een lokale computer of in een werkgroep of domein.

noodherstelarchief Een beschermde opslagplaats waarmee primaire gebruikerssleutels opnieuw kunnen worden gecodeerd van de ene Platform Owner Key naar de andere.

opschonen van vrije ruimte Het overschrijven van verwijderde gegevensbestanddelen met willekeurige gegevens om de inhoud van het verwijderde gegevensbestanddeel onleesbaar te maken.

opstartverificatie Een beveiligingsvoorziening die ervoor zorgt dat een gebruiker zich moet verifiëren wanneer de computer wordt ingeschakeld, met behulp van bijvoorbeeld een Java Card, beveiligingschip of wachtwoord.

pincode Persoonlijk identificatienummer (PIN)

PKI Public Key Infrastructure, een standaard die de interfaces definieert voor het maken, gebruiken en beheren van certificaten en cryptografische sleutels.

Privacy Manager-certificaat Een digitaal certificaat dat verificatie vereist telkens wanneer u het gebruikt voor cryptografische bewerkingen, zoals het ondertekenen en coderen van e-mailberichten en Microsoft Office-documenten.

PSD Personal secure drive. Biedt een beveiligde opslagruimte voor gevoelige informatie.

referenties Gegevens waarmee een gebruiker tijdens het verificatieproces aantoont dat hij of zij gemachtigd is voor het uitvoeren van een bepaalde taak.

SATA apparaatmodus Modus voor gegevensoverdracht tussen een computer en apparaten voor massaopslag, zoals vaste schijven en optischeschijfeenheden.

Scène Een foto van een geregistreerde gebruiker die wordt gebruikt voor verificatie.

Send Securely (Veilig verzenden) Een knop in de software die op de werkbalk van e-mailberichten in Microsoft Outlook staat. Als u op deze knop klikt, kunt u e-mailberichten in Microsoft Outlook ondertekenen en/of coderen.

sessie in chatgeschiedenis Een gecodeerd bestand waarin beide kanten van een conversatie in een chatsessie staan geregistreerd.

Sign and Encrypt (Ondertekenen en coderen) Een knop in de software die op de werkbalk van e-mailberichten in Microsoft Office staat. Als u op deze knop klikt, kunt u een Microsoft Office-document onderteken, coderen of de codering verwijderen.

Single sign-on (Eenmalige aanmelding) Een voorziening waarmee verificatiegegevens worden opgeslagen en waarmee met Security Manager toegang kan worden verkregen tot internet- en Windows-applicaties waarvoor wachtwoordverificatie vereist is.

smart card Een kleine kaart met het formaat van een bankpas, waarop identificatiegegevens van de eigenaar zijn opgeslagen. Deze kunnen worden gebruikt voor verificatie op een computer.

terugzetten Een proces waarbij programmagegevens uit een eerder opgeslagen back-upbestand worden gekopieerd naar dit programma.

toetscombinatie Een combinatie van bepaalde toetsen waarmee u een automatische versnipperingsactie in gang zet, bijvoorbeeld ctrl+alt+s.

token Zie beveiligingsaanmeldmethode.

TXT Trusted Execution Technology.

uitnodiging voor vertrouwde contactpersoon Een e-mailbericht dat naar een persoon wordt verzonden met de vraag om een vertrouwde contactpersoon te worden.

USB-token Beveiligingsvoorziening die identificatiegegevens van een gebruiker opslaat. Net als een Java Card of een biometrische lezer wordt een USB-token gebruikt om de bezitter van een computer te verifiëren.

verificatie Proces waarbij wordt gecontroleerd of een gebruiker toestemming heeft om een bepaalde taak uit te voeren, zoals toegang tot een computer krijgen, instellingen voor een bepaald programma wijzigen of beveiligde gegevens bekijken.

versnipperen De uitvoering van een algoritme dat de gegevens in een gegevensbestanddeel onleesbaar maakt.

versnipperingscyclus Het aantal keren dat het versnipperingsalgoritme wordt uitgevoerd voor elk gegevensbestanddeel. Hoe hoger het aantal versnipperingscycli dat u instelt, hoe veiliger de computer is.

versnipperingsprofiel Een geselecteerde wismethode en een lijst met gegevensbestanddelen.

vertrouwd bericht Een communicatiesessie waarbij vertrouwde berichten worden verzonden van een vertrouwde afzender naar een vertrouwde contactpersoon.

vertrouwde afzender Een vertrouwde contactpersoon die ondertekende en/of gecodeerde e-mailberichten en Microsoft Office-documenten verzendt.

vertrouwde contactpersoon Een persoon die een uitnodiging om een vertrouwde contactpersoon te worden heeft aanvaard.

vertrouwde contactpersoon als ontvanger Een persoon die een uitnodiging ontvangt om een vertrouwde contactpersoon te worden.

vertrouwde IM-communicatie Een communicatiesessie waarbij vertrouwde berichten worden verzonden van een vertrouwde afzender naar een vertrouwde contactpersoon.

verzegelen voor vertrouwde contactpersonen Een taak die een digitale handtekening toevoegt, het e-mailbericht codeert en het verstuurt nadat u een verificatie heeft uitgevoerd met de door u gekozen beveiligde aanmeldingsmethode.

vingerafdruk Een digitale versie van de afbeelding van uw vingerafdruk. De feitelijke afbeelding van uw vingerafdruk wordt nooit door Security Manager opgeslagen.

virtueel token Beveiligingsvoorziening die werkt op een manier die vergelijkbaar is met een Java Card en een kaartlezer. Het token wordt opgeslagen op de vaste schijf van de computer of in het Windows-register. Wanneer u zich aanmeldt met een virtueel token, wordt u om een gebruikerspincode gevraagd om de verificatie te voltooien.

voorgestelde ondertekenaar Een gebruiker die door de eigenaar van een Microsoft Word- of Microsoft Excel-document wordt aangewezen om een handtekeningregel aan het document toe te voegen

wachtwoord voor intrekking Een wachtwoord dat wordt gemaakt wanneer een gebruiker een digitaal certificaat aanvraagt. Het wachtwoord is vereist wanneer de gebruiker zijn of haar digitale certificaat wil intrekken. Dit garandeert dat alleen de gebruiker het certificaat kan intrekken.

Windows-beheerder Een gebruiker met volledige rechten om toegangsmachtigingen te wijzigen en andere gebruikers te beheren.

Windows-gebruikersaccount Een profiel voor een persoon die is gemachtigd om zich aan te melden bij een netwerk of op een bepaalde computer.

zichtbaar maken Een taak die de gebruiker in staat stelt een of meer sessies uit de chathistorie te decoderen, waardoor de schermnaam van de contactpersoon of contactpersonen in gewone tekst wordt weergegeven en de sessie beschikbaar is voor weergave.

Index