HP Client Security

Aan de slag

Eerste editie: augustus 2013

Artikelnummer van document: 735339-331

Inhoudsopgave

1 Inleiding tot HP Client Security Manager

Met HP Client Security kunt u uw gegevens, apparaat en identiteit beschermen, waardoor u de beveiliging van uw computer verbetert.

De software - modules die voor uw computer beschikbaar zijn, kunnen variëren afhankelijk van uw model.

Modules van HP Client Security-software kunnen vooraf zijn geïnstalleerd, voorgeladen; of beschikbaar voor downloaden van de HP website. raadpleeg http://www.hp.com voor meer informatie.

OPMERKING: De instructies in deze handleiding zijn geschreven met als uitgangspunt dat u de betreffende modules voor de HP Client Security-software al geïnstalleerd hebt.

Functies van HP Client Security

De volgende tabel beschrijft de voornaamste functies van de modules van HP Client Security modules.

Module	Belangrijkste functies
HP Client Security Manager	Beheerders kunnen de volgende functies uitvoeren: • Uw computer beveiligen voordat Windows® start • Uw Windows-account te beschermen met sterke verificatie • Uw aanmelding en wachtwoorden voor websites en applicaties beheren • Gemakkelijk het wachtwoord veranderen van uw Windows besturingssysteem • Vingerafdrukken gebruiken voor extra beveiliging en gemak • Een smartcard, contactloze kaart of nabijheidskaart instellen voor verificatie • Uw Bluetooth-telefoon gebruiken als een manier van verificatie • Een pincode instellen om de verificatiemoogelijkheden uit te breiden • Beleiden voor aanmelden en sessies instellen • Back-ups van programmagegevens maken en deze herstellen • Meer applicaties toevoegen, zoals HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager en HP Computrace Algemene gebruikers kunnen de volgende functies uitvoeren: • INstellingen voor de Coderingsstatus en Device Access Manager bekijken. • Computrace activeren. • Voorkeuren en Backup en herstelopties instellen.
Password Manager	Algemene gebruikers kunnen de volgende functies uitvoeren: • Gebruikersnamen en wachtwoorden organiseren en instellen. • Krachtiger wachtwoorden maken voor een betere accountbeveiliging voor e-mail en webaccounts. Password Manager vult de gegevens automatisch in en biedt deze aan. • Stroomlijn het aanmeldproces met de functie Single Sign On, die automatisch gebruikersgegevens onthoudt en toepast. • Een account als gecompromitteerd markeren zodat u wordt gewaarschuwd voor ander account(s) met vergelijkbare referenties. • Importeren van aanmeldgegevens van een ondersteunde browser.
HP Drive Encryption (alleen bepaalde modellen)	• Biedt volledige, full-volume codering van de vaste schijf. • Dwingt pre-boot authenticatie af om de gegevens te decoderen en toegankelijk te maken. • Biedt de optie om zelf-coderende stations te activeren (alleen bepaalde modellen).

Module	Belangrijkste functies
HP Device Access Manager	• Maakt het IT-managers mogelijk om de toegang tot apparaten te regelen op basis van gebruikersprofielen. • Verhindert dat onbevoegde gebruikers gegevens verwijderen via externe opslagmedia en voorkomt introductie van virussen in het systeem vanaf externe media. • Beheerders kunnen toegang uitschakelen tot communicatieapparaten voor bepaalde personen of groepen van gebruikers.
HP Trust Circles	• Biedt bestand- en documentbeveiliging. • Codeert bestanden geplaatst in door de gebruiker opgegeven mappen en beschermt ze binnen een trust circle • Maakt het mogelijk om bestanden alleen door leden van de trust circle te laten gebruiken en delen.
Herstel na diefstal (Computrace, afzonderlijk aan te schaffen)	• Vereist afzonderlijke aanschaf van opsporings- en traceerabonnementen om te activeren. • Biedt beveiligde activaregistratie. • Bewaakt de activiteiten van de gebruiker, alsmede wijzigingen in hardware en software. • Blijft zelfs actief na het formateeren of vervangen van de harde schijf.

Productbeschrijving HP Client Security en veelvoorkomende gebruiksvoorbeelden

De meeste HP Client Security-producten gebruiken zowel verificatie van de gebruiker (meestal een wachtwoord) en een administratieve back-up om toegang te krijgen als wachtwoorden verloren zijn, niet beschikbaar zijn of vergeten zijn, of wanneer de bedrijfsbeveiliging toegang nodig heeft.

OPMERKING: Enkele van de HP Client Security-producten zijn ontworpen om toegang tot gegevens te beperken. Gegevens moeten gecodeerd zijn als ze zo belangrijk zijn dat de gebruiker liever de informatie kwijtraakt dan deze te compromitteren. Aangeraden wordt om van alle gegevens een back-up te maken op een veilige plaats.

Password Manager

Password Manager slaat gebruikersnamen en wachtwoorden op en kan worden gebruikt voor:

- Opslaan van aanmeldnamen en wachtwoorden voor toegang tot internet of e-mail .
- De gebruiker automatisch aanmelden bij een website of e-mail .
- Verificaties beheren en organiseren.
- Selecteren van een Web- of network-activa en rechtstreeks toegang krijgen tot de koppeling.
- Bekijken van namen en wachtwoorden wanneer dit nodig is.
- Een account als gecompromitteerd markeren zodat u wordt gewaarschuwd voor ander account(s) met vergelijkbare referenties.
- Importeren van aanmeldgegevens van een ondersteunde browser.

Voorbeeld 1: Een inkoopagent voor een grote fabrikant voert het grootste deel van haar zakelijke transacties via internet uit. Zij bezoekt ook regelmatig verschillende populaire websites die aanmeldgegevens vereisen. Zij is zich scherp bewust van beveiliging dus ze gebruikt nooit hetzelfde wachtwoord op elke account. De inkoopagent heeft besloten om Password Manager te gebruiken om webkoppelingen met verschillende gebruikersnamen en wachtwoorden op elkaar af te stemmen. Als ze naar een website gaat om zich aan te melden, presenteert Password Manager de referenties automatisch. Als zij de gebruikersnamen en wachtwoorden wil bekijken, kan Password Manager worden ingesteld om ze weer te geven.

Password Manager kan ook worden gebruikt om de verificaties te beheren en te organiseren. Met dit hulpmiddel kan een gebruiker Web- of netwerkactiva selecteren en direct toegang tot de koppeling krijgen. Bovendien kan de gebruiker de gebruikersnamen en wachtwoorden weergeven wanneer dat nodig is.

Voorbeeld 2: Een hardwerkende werknemer is gepromoveerd en gaat nu de gehele boekhoudafdeling beheren. Het team moet zich aanmelden op een groot aantal webaccounts van clients, die elk andere aanmeldgegevens gebruiken. Deze aanmeldgegevens moeten worden gedeeld met andere werknemers, zodat vertrouwelijkheid een belangrijk punt is. De werknemer besluit om alle koppelingen naar websites, bedrijfsgebruikersnamen en wachtwoorden binnen Password Manager te organiseren. Zodra de werknemer klaar is, implementeert hij Password Manager voor de werknemers zodat ze met de webaccounts kunnen werken en nooit de aanmeldingsgegevens weten die ze gebruiken.

HP Drive Encryption (alleen bepaalde modellen)

HP Drive Encryption wordt gebruikt om de toegang te beperken tot de gegevens op de gehele harde schijf van de computer of op een secundaire schijf. Drive Encryption kan ook zelf-coderende schijfeenheden beheren.

Voorbeeld 1: Een arts wil er voor zorgen dat alleen hij toegang heeft tot alle gegevens op de vaste schijf van zijn computer. De arts activeert Drive Encryption waarvoor verificatie voorafgaand aan opstarten nodig is voorafgaand aan de Windows-aanmelding. Eenmaal ingesteld, kan de harde schijf niet gebruikt worden zonder het wachtwoord voordat het besturingssysteem is gestart. De arts zou de schijfeenheid verder kunnen beveiligen door te kiezen om de gegevens te coderen met de zelf-coderende schijfoptie.

Voorbeeld 2: Een netwerkbeheerder op een ziekenhuis wil er voor zorgen dat alleen artsen en geautoriseerd personeel toegang krijgen tot gegevens op hun lokale computer zonder hun persoonlijke wachtwoorden te delen. De IT-afdeling voegt de beheerder, artsen en alle geautoriseerde medewerkers toe als gebruiker van Drive Encryption. Nu kan alleen geautoriseerd personeel de computer of het domein opstarten met hun persoonlijke gebruikersnaam en wachtwoord.

HP Device Access Manager (alleen bepaalde modellen)

Met HP Device Access Manager kan een beheerder de toegang tot hardware beperken en beheren. HP Device Access Manager kan ongeoorloofde toegang tot USB-sticks waar gegevens kunnen worden gekopieerd. Het kan ook de toegang beperken tot cd-/dvd-stations, bediening van USB-apparaten, netwerkverbindingen, enzovoort. Een voorbeeld is een situatie waarin externe leveranciers toegang nodig hebben tot bedrijfscomputers maar de gegevens niet mogen kopiëren naar een USB-station.

Voorbeeld 1: Een manager van een bedrijf voor medische artikelen werkt vaak met persoonlijke medische gegevens samen met zijn bedrijfsinformatie. De medewerkers hebben toegang tot deze gegevens nodig, maar het is echter uiterst belangrijk dat de gegevens niet vanaf de computer worden verwijderd met een USB-schijfeenheid of een ander extern opslagmedium. Het netwerk is bveilig maar de computers hebben CD-branders en USB-poorten die het mogelijk kunnen maken dat de

gegevens worden gekopieerd of gestolen. De manager gebruikt Device Access Manager om de USB-poorten en CD branders uit te schakelen, zodat deze niet kunnnen worden gebruikt. Hoewel de USB-poorten zijn geblokkeerd, kunnen muis en toetsenbord nog steeds gebruikt worden.

Voorbeeld 2: Een verzekeringsmaatschappij wil niet dat werknemers persoonlijke software of gegevens van thuis installeren of plaatsen. Sommige werknemers hebben toegang nodig tot een USB-poort op alle computers. De IT-manager gebruikt Device Access Manager om toegang in te schakelen voor sommige werknemers en externe toegang voor andere te blokkeren.

Computrace (afzonderlijk aan te schaffen)

Computrace (afzonderlijk aan te schaffen) is een service die de locatie van een gestolen computer kan volgen wanneer de gebruiker het internet benadert. Computrace kan ook helpen bij het beheer op afstand en het zoeken naar computers, alsmede het computergebruik en toepassingen bewaken.

Voorbeeld 1: Een schoolhoofd heeft de IT-afdeling opgedragen om alle cmputers op de school bij te houden. Nadat de inventaris van de computers is gemaakt, heeft de IT-beheerder alle computers met Computrace geregistreerd zodat ze kunnen worden opgespoord in het geval ze ooit worden gestolen. Onlangs ontdekte de school dat meerdere computers ontbraken, zodat de IT-beheerder de autoriteiten en de Computrace-ambtenaren heeft gewaarschuwd. De computers werden gelokaliseerd en door de autoriteiten naar de school teruggezonden.

Voorbeeld 2: Een onroerendgoedmaatschappij moet computers overal ter wereld beheren en bijwerken. Ze gebruiken Computrace om de computers te bewaken en bij te werken zonder een IT personen naar elke computer te sturen.

Belangrijke beveiligingsdoelstellingen bereiken

HP Client Security-modules kunnen samenwerken om oplossingen voor tal van beveiligingsproblemen te bieden, waaronder de volgende belangrijke beveiligingsdoelstellingen:

- Bescherming tegen gerichte diefstal
- Beperking van de toegang tot gevoelige gegevens
- Ongeoorloofde toegang voorkomen vanaf interne of externe locaties
- Beleiden instellen voor sterke wachtwoorden

Bescherming tegen gerichte diefstal

Een voorbeeld van doelgerichte diefstal is de diefstal van een computer met vertrouwelijke gegevens en informatie voor de klant bij een controlepunt voor beveiliging op een vliegveld. De volgende functies helpen beschermen tegen gerichte diefstal:

- De functie verificatie voorafgaand aan opstarten, als deze is ingeschakeld, helpt toegang tot het besturingssysteem te voorkomen.
  - HP Client Security—zie HP Client Security op pagina 13.
  - HP Drive Encryption—zie HP Drive Encryption (alleen bepaalde modellen) op pagina 31.
- Codering helpt ervoor zorgen dat gegevens niet toegankelijk zijn zelfs als de harde schijf is verwijder en in een niet-beveiligd systeem is geplaatst.
- Computrace kan de locatie van een computer na een diefstal traceren.
  - Computrace—zie Theft recovery (alleen bepaalde modellen) op pagina 56.

Beperking van de toegang tot gevoelige gegevens

Stel dat een contractcontroleur op locatie werkt en toegang heeft gekregen tot een computer voor de beoordeling van gevoelige financiële gegevens. U wilt niet de accountant de bestanden kan afdrukken of opslaan op een beschrijfbare apparaat, zoals de CD. De volgende functie helpt bij het beperken van de toegang tot gegevens:

- HP Device Access Manager staat IT-managers toe om de toegang tot communicatie-apparaten te beperken zodat gevoelige informatie niet vanaf de harde schijf gekopieerd kan worden. Zie Systeemweergave op pagina 45.

Ongeoorloofde toegang voorkomen vanaf interne of externe locaties

Ongeoorloofde toegang tot een niet-beveiligde zakelijke computer is een daadwerkelijk risico voor bedrijfsnetwerkbronnen zoals informatie van financiële diensten, een directeur, of het onderzoek en ontwikkelingsteam, en voor privé-informatie zoals patiëntgegevens of persoonlijke financiële records. De volgende functies helpen ongeoorloofde toegang voorkomen:

- De functie verificatie voorafgaand aan opstarten, als deze is ingeschakeld, helpt toegang tot het besturingssysteem te voorkomen. (zie HP Drive Encryption (alleen bepaalde modellen) op pagina 31.
- HP Client Security helpt ervoor te zorgen dat een onbevoegde gebruiker geen wachtwoorden kan ophalen of toegang krijgen tot met een wachtwoord beveiligde toepassingen. Zie HP Client Security op pagina 13.
- HP Device Access Manager staat IT-managers toe om de toegang tot beschrijfbare apparaten te beperken zodat gevoelige informatie niet vanaf de harde schijf gekopieerd kan worden. Zie HP Device Access Manager (alleen bepaalde modellen) op pagina 44.

Beleiden instellen voor sterke wachtwoorden

Als een bedrijfsbeleid van kracht wordt dat het gebruik van sterk wachtwoordbbeleiden vereist voor tientallen webapplicaties en databases, Password Manager een beveiligde opslagplaats voor wachtwoorden en Single Sign On-gemak. Zie Password Manager op pagina 19.

Extra beveiligingselementen

Toewijzen veiligheidsrollen

Bij het beheren van computerbeveiliging (met name voor grote organisaties) is een belangrijke gewoonte het verdelen van verantwoordelijkheden en rechten over verschillende soorten beheerders en gebruikers.

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

Voor HP Client Security kunnen de beveiligingstaken en rechten over de volgende rollen worden verdeeld:

- Beveiligingsverantwoordelijke: definieert het beveiligingsniveau voor het bedrijf of netwerk en bepaalt de te implementeren beveiligingsfuncties, zoals Drive Encryption.

OPMERKING: Veel van de functies in HP Client Security kunnen worden aangepast door de beveiligingsverantwoordelijke in samenwerking met HP. raadpleeg http://www.hp.com voor meer informatie.

- IT-beheerder: past de beveiligingsfuncties toe die zijn gedefinieerd door de beveiligingsverantwoordelijke en beheert deze. Kan ook sommige functies in- en uitschakelen. Als bijvoorbeeld de beveiligingsverantwoordelijke besloten heeft om smart cards te implementeren, kan de IT-beheerder zowel de wachtwoord- als de smartcard-modus inschakelen.
- Gebruiker: gebruikt de beveiligingsvoorzieningen. Als bijvoorbeeld de beveiligingsverantwoordelijke en de IT-beheerder smartcards voor het systeem hebben ingeschakeld, kan de gebruiker de PIN-code voor de smartcard instellen en de kaart voor verificatie gebruiken.

VOORZICHTIG: Beheerders worden aangemoedigd om "best practices" te volgen bij het beperken van de bevoegdheden van eindgebruikers en het beperken van gebruikerstoegang.

Ongeoorloofde gebruikers moeten geen beheerdersrechten worden verleend.

Beheren van HP Client Security wachtwoorden

De meeste functies van HP Client Security worden door wachtwoorden beveiligd. De volgende tabel geeft een overzicht van de gewoonlijk gebruikte wachtwoorden, de softwaremodule waar het wachtwoord is ingesteld en de wachtwoordfunctie.

De wachtwoorden die alleen door IT-beheerders worden ingesteld en gebruikt, zijn in deze tabel ook aangegeven. Alle andere wachtwoorden kunnen worden ingesteld door regelmatige gebruikers of beheerders.

HP Client Security wachtwoord	Ingesteld in de volgende module	Functie
Windows-wachtwoord	Configuratiescherm van Windows of HP Client Security	Dit kan worden gebruikt voor handmatige aanmelding en voor verificatie om toegang te krijgen tot verschillende voorzieningen van HP Client Security.
Wachtwoord voor HP Client Security Back-up en Recovery	HP Client Security, door individuele gebruiker	Beveiligt de toegang tot het HP Client Security Back-up en Recovery-bestand.
Pincode van smartcard	Credential Manager	Kan als multifactor-verificatie worden gebruikt. Kan als Windows-verificatie worden gebruikt. Verifieert gebruikers van Drive Encryption als de smartcard is geselecteerd.

Het maken van een beveiligd wachtwoord

Bij het maken van wachtwoorden moet u eerst eventuele specificaties volgen die door het programma zijn ingesteld. In het algemeen moet u echter de volgende richtlijnen overwegen om u te

helpen bij het maken van sterke wachtwoorden en het beperken van de kans dat uw wachtwoord in gevaar wordt gebracht:

- Gebruik wachtwoorden met meer dan 6 tekens, bij voorkeur meer dan 8.
- Gebruik zowel hoofd- als kleine letters in uw wachtwoord.
- Vermeng waar mogelijk alfanumerieke tekens en neem speciale tekens en leestekens op.
- Vervang speciale tekens of nummers door letters in een sleutelwoord. U kunt bijvoorbeeld het nummer 1 voor de letters I of L gebruiken.
- Combineer woorden uit 2 of meer talen.
- Splits een woord of zin met cijfers of speciale tekens in het midden, bijvoorbeeld "Mary2-2Cat45."
- Gebruik geen wachtwoord dat in een woordenboek kan voorkomen.
- Gebruik niet uw eigen naam als wachtwoord, of andere persoonlijke informatie, zoals uw geboortedatum, de naam van uw huisdier, of de meisjesnaam van uw moeder, zelfs als u het achterstevoren spelt.
- Wijzig wachtwoorden regelmatig. U hoeft bijvoorbeeld alleen maar enkele tekens te verhogen.
- Als u uw wachtwoord noteert, sla het dan niet op in een goed zichtbare plaats vlakbij de computer.
- Sla het wachtwoord niet op de computer op in een bestand, zoals een e-mail.
- Deel geen accounts en vertel niemand uw wachtwoord.

Een back-up maken van referenties en instellingen

U kunt het hulpmiddel Back-up en Recovery in HP Client Security gebruiken als een centrale locatie waar u een back-up kunt maken van beveiligingsreferenties en deze kunt herstellen van enkele van de geïnstalleerde HP Client Security-modules.

2 Aan de slag

Om HP Client Security in te stellen met uw referenties, start u HP Client Security op een van de volgende manieren: Zodra de wizard door een gebruiker is voltooid, kan deze niet opnieuw door de gebruiker worden gestart.

1. Klik of tik op het start- of apps-scherm op de app **HP Client Security** (Windows 8).

   – of –

   Klik of tik op het bureaublad van Windows op de app **HP Client Security Gadget** (Windows 7).

   – of –

   Dubbelklik of dubbeltik op het bureaublad van Windows op het pictogram **HP Client Security** in het systeemvak, rechts op de taakbalk.

   – of –

   Dubbelklik of dubbeltik op het bureaublad van Windows op het pictogram **HP Client Security** in het systeemvak, rechts op de taakbalk en selecteer **Open HP Client Security**.

2. De HP Client Security Setup wizard start en de welkomstpagina verschijnt.

3. Lees het welkomstscherm, verifieer uw identiteit door uw Windows-wachtwoord te typen, en klik of tik op **Volgende**.

   Als u nog geen Windows-wachtwoord hebt ingesteld, wordt u hiertoe uitgenodigd. Een Windows-wachtwoord is vereist om uw Windows-account te beschermen tegen toegang door niet-geautoriseerde personen en om de fucnties van HP Client Security te gebruiken.

4. Selecteer drie beveiligingsvragen op de pagina HP SpareKey. Voer voor elke vraag een antwoord in en klik op **Volgende**. Ook aangepaste vragen zijn toegestaan. Zie HP SpareKey - wachtwoord terugzetten op pagina 15 voor meer informatie.

5. Registreer op de pagina Fingerprints (vingerafdrukken) in elk geval het minimale aantal vereiste vingerafdrukken en klik of tik op **Volgende**. Zie Vingerafdrukken op pagina 13 voor meer informatie.

6. Activeer op de pagina Drive Encryption de codering, maak een back-up van de coderingssleutel en klik of tik op **Volgende** Zie de Help voor de HP Drive Encryption software voor meer informatie.

OPMERKING: Dit is van toepassing op een scenario waarbij de gebruiker een beheerder is en de HP Client Security Setup wizard nog niet eerder is ingesteld door een beheerder.

7. Klik of tik op de laatste pagina van de wizard op **Voltooien**.

   Deze pagina toont de status van functies en referenties.

8. De HP Client Security Setup wizard zorgt voor de activering van de functies Just In Time Authentication en File Sanitizer. Zie voor meer informatie de HP Device Access Manager software Help en de HP File Sanitizer software Help.

OPMERKING: Dit is van toepassing op een scenario waarbij de gebruiker een beheerder is en de HP Client Security Setup wizard nog niet eerder is ingesteld door een beheerder.

HP Client Security openen

U kunt de applicatie HP Client Security op een van de volgende manieren openen:

OPMERKING: De HP Client Security Setup Wizard moet zijn voltooid voordat de applicatie HP Client Security kan starten.

- Klik of tik op het start- of apps-scherm op de app **HP Client Security**.

  – of –

  Klik of tik op het bureaublad van Windows op de app **HP Client Security Gadget** (Windows 7).

  – of –

  Dubbelklik of dubbeltik op het bureaublad van Windows op het pictogram **HP Client Security** in het systeemvak, rechts op de taakbalk.

  – of –

  Dubbelklik of dubbeltik op het bureaublad van Windows op het pictogram **HP Client Security** in het systeemvak, rechts op de taakbalk en selecteer **Open HP Client Security**.

3 Easy Setup Handleiding voor kleine bedrijven

In dit hoofdstuk worden de basisstappen gedemonstreerd voor het activeren van de meest voorkomende en nuttigste opties binnen HP Client Security voor kleine bedrijven. Met talloze hulpmiddelen en opties in deze software kunt u uw voorkeuren afstemmen en uw toegangsbeheer instellen. Deze Easy Setup Handleiding is er op gericht om elke module uit te voeren met minimale inspanningen en tijd voor het instellen. Voor extra informatie selecteert u de module waarin u geïnteresseerd bent en klikt u op de **?** of knop Help in de rechter bovenhoek. Deze knop toont automatisch informatie om u te helpen met het momenteel weergegeven venster.

Aan de slag

1. Dubbelklik of dubbeltik op het bureaublad van Windows op het pictogram **HP Client Security** in het systeemvak, rechts op de taakbalk om HP Client Security te openen.
2. Typ uw Windows-wachtwoord of maak een Windows-wachtwoord.
3. Voltooi de installatie van HP Client Security.

Om HP Client Security om slechts eenmaal tijdens de Windows-aanmelding om verificatie te vragen, zie Beveiligingfuncties op pagina 28.

Password Manager

Iedereen heeft een groot aantal wachtwoorden - met name als u regelmatig websites of toepassingen gebruikt waarvoor u zich moet aanmelden. De normale gebruiker gebruikt of hetzelfde wachtwoord voor elke toepassing en website of wordt creatief en vergeet meteen welk wachtwoord bij welke toepassing hoort.

Password Manager kan automatisch uw wachtwoorden onthouden of u de mogelijkheid geven om vast te stellen welke sites onthouden moeten worden en welke niet. Als u zich aanmeldt bij de computer, biedt Password Manager u de wachtwoorden of referenties aan voor deelname aan toepassingen of websites.

Wanneer u een toepassing of website opent waarvoor referenties nodig zijn, herkent Password Manager automatisch de website en vraagt het u of wilt dat de software uw gegevens onthoudt. Als u bepaalde sites wilt uitsluiten, kunt u het verzoek weigeren.

Beginnen met sparen van weblocaties, gebruikersnamen en wachtwoorden:

1. Navigeer voorbeeld naar een deelnemende website of toepassing en klik vervolgens op het pictogram van Password Manager in de linkerbovenhoek van de webpagina om de webverificatie toe te voegen.
2. Geef de koppeling een naam (optioneel) en voer een gebruikersnaam en wachtwoord in Password Manager in.
3. Als u klaar bent, klikt u op de knop **OK**.
4. Password Manager kan ook uw gebruikersnaam en wachtwoorden voor netwerk-shares of gekoppelde netwerkschijven opslaan.

De opgeslagen verificaties in Password Manager bekijken

In Password Manager kunt u uw verificaties bekijken, beheren, back-ups maken, en starten vanuit een centrale locatie. Password Manager ondersteunt ook het starten van opgeslagen locaties vanuit Windows.

Om Password Manager te openen, gebruikt u de toetsenbordcombinatie Ctrl+Windows-toets+h om Password Manager te openen, waarna u op **Aanmelden** klikt om de opgeslagen snelkoppeling te starten en verifiëren.

Met de optie **Bewerken** van Password Manager kunt u de naam en aanmeldnaam bekijken en bewerken en zelfs de wachtwoorden zichtbaar maken.

Met HP Client Security for Small Business kunt u van alle referenties en instellingen een back-up maken en/of kopiëren naar een andere computer.

HP Device Access Manager

U kunt Device Access Manager gebruiken bij het beperken van het gebruik van diverse interne en externe opslagapparaten, zodat uw gegevens beveiligd blijven op de vaste schijf en niet het bedrijf verlaten. Een voorbeeld hiervan is een gebruiker toegang bieden tot uw gegevens, maar verhinderen dat deze ze naar een cd, persoonlijke muziekspeler of USB-geheugenapparaat kopieert.

1. Open **Device Access Manager** (zie Device Access Manager openen op pagina 45).

   De toegang voor de huidige gebruiker wordt weergegeven.

2. Om de toegang voor gebruikers, groepen of apparaten te wijzigen, klikt of tikt u op **Wijzigen**. Zie Systeemweergave op pagina 45 voor meer informatie.

HP Drive Encryption

HP Drive Encryption wordt gebruikt om uw gegevens te beschermen door de gehele harde schijf te coderen. De gegevens op uw harde schijf blijven beschermd als uw PC ooit wordt gestolen en/of als de vaste schijf uit de originele computer wordt verwijderd en in een andere computer geplaatst.

Een extra beveiligingsvoordeel is Drive Encryption vereist dat u zich goed verifieert met uw gebruikersnaam en wachtwoord voordat het besturingssysteem start. Dit proces heet verificatie voorafgaand aan opstarten.

Om het u gemakkelijk te maken, synchroniseren meerdere softwaremodules wachtwoorden automatisch, inclusief Windows gebruikersaccounts, verificatiedomeinen, HP Drive Encryption, Password Manager en HP Client Security.

Voor het instellen van HP Drive Encryption tijdens de eerste installatie met de installatiewizard voor HP Client Security, zie Aan de slag op pagina 9.

4 HP Client Security

De startpagina van HP Client Security is de centrale locatie voor eenvoudige toegang tot de functies, applicaties en instellingen van HP Client Security. De startpagina is onderverdeeld in drie secties:

- **DATA**: biedt toegang tot applicaties gebruikt voor het beheer van gegevensbeveiliging.
- **DEVICE**: biedt toegang tot applicaties gebruikt voor het beheer van de beveiliging van het apparaat.
- **IDENTITY**: biedt registratie en beheer van verificatiereferenties.

Ga met de cursor naar een applicatietegel om een beschrijving van de applicatie weer te geven.

HP Client Security kan onderaan een pagina koppelingen bevatten naar gebruikers- en beheerdersinstellingen. HP Client Security biedt toegang tot geavanceerde instellingen en functies door op het pictogram **Tandwiel** (instellingen) te klikken of tikken.

Identiteitsfuncties, applicaties en instellingen

De identiteitsfuncties, applicaties en instellingen die geleverd worden door HP Client Security helpen u bij het beheren van verschillende aspecten van uw digitale identiteit. Klik of tik op de volgende tegels op de startpagina van HP Client Security en voer uw Windows-wachtwoord in.

- **Fingerprints** (Vingerafdrukken): registreer en beheer uw vingerafdrukken.
- **SpareKey**: stelt uw HP SpareKey-referentie in en beheert deze, die u kunt gebruiken om u aan te melden bij uw computer als andere referenties verloren zijn. Hiermee kunt u tevens een vergeten wachtwoord opnieuw instellen.
- **Windows Password** (Windows-wachtwoord): biedt eenvoudige toegang voor het veranderen van uw Windows-wachtwoord.
- **Bluetooth Devices** (Bluetooth-apparaten): hiermee kunt u uw Bluetooth-apparaten registreren en beheren.
- **Cards** (Kaarten): hiermee kunt u uw smartcards, contactloze kaarten en nabijheidskaarten registreren en beheren.
- **PIN**: hiermee kunt u uw PIN-referentie registreren en beheren.
- **RSA Securid**: hiermee kunt u uw RSA Securid referentiegegevens opgeven en beheren (indien de betreffende installatie aanwezig is).
- **Password Manager** (Wachtwoordbeheer): hiermee kunt u wachtwoorden beheren voor uw online accounts en applicaties.

Vingerafdrukken

De HP Client Security Setup Wizard begeleidt u bij het instellen of "registreren" van uw vingerafdrukken.

U kunt uw vingerafdrukken ook registreren of verwijderen op de pagina Fingerprints die u opent door op het pictogram **Vingerafdrukken** te klikken of tikken op de startpagina van HP Client Security.

1. Veeg een vinger op de pagina Fingerprints tot deze is geregistreerd.

   Het voor registratie vereiste aantal vingerafdrukken is op de pagina aangegeven. De voorkeur gaat uit naar wijs- of middelvingers.

2. Klik of tik op **Verwijderen** om eerder geregistreerde vingerafdrukken te verwijderen.
3. Klik of tik op **Enroll an additional fingerprint** (Een extra vingerafdruk registreren) als u meer vingerafdrukken wilt registreren.
4. Klik of tik op **Opslaan** voordat u de pagina sluit.

⚠ **VOORZICHTIG:** Bij het registreren van vingerafdrukken met de wizard wordt infomatie over de vingerafdrukken pas opgeslagen als u op **Volgende** klikt. Als u de computer een tijdje niet gebruikt of u sluit het programma, worden de aangebrachte wijzigingenare **niet** opgeslagen.

- Om de Fingerprints Administrative Settings (Beheerinstellingen voor Vingerafdrukken) te openen waar beheerders de registratie, nauwkeurigheid en andere instellingen kunnen opgeven, klikt of tikt u op **Administrative Settings** (Beheerinstellingen) (vereist beheerdersbevoegdheden).
- Om de Fingerprints User Settings (Gebruikersinstellingen voor Vingerafdrukken) te openen waar u instellingen kunt opgeven die het uiterlijk en de werking van de vingerafdrukherkenning bepalen, klikt of tikt u op **User Settings** (Gebruikersinstellingen).

Fingerprints Administrative Settings (Beheerinstellingen voor Vingerafdrukken)

Beheerders kunnen de registratie, nauwkeurigheid en andere instellingen voor een vingerafdruklezer instellen. Hiervoor zijn beheerdersbevoegdheden vereist.

- Klik op de pagina Fingerprints op **Administrative Settings** (Beheerinstellingen) om de Beheerinstellingen voor de vingerafdrukreferenties te openen.

- **User enrollment** (Registratie gebruiker): kies het minimale en maximale aantal vingerafdrukken dat een gebruiker mag registreren.
- **Recognition** (Herkenning): verplaats de schuif om de gevoeligheid van de vingerafdruklezer in te stellen als u uw vinger veegt.

  Als uw vingerafdruk niet consistent herkend wordt, moet u mogelijk een lagere herkenningsinstelling kiezen. Een hogere instelling verhoogt de gevoeligheid bij het vegen van vingerafdrukken en verlaagt daardoor de kans op een onjuiste acceptatie. De instelling **Medium-High** (Gemiddeld-Hoog) vormt een goede mix van beveiliging en gemak.

Fingerprints User Settings (Gebruikersinstellingen voor Vingerafdrukken)

Op de pagina Fingerprint User Settings (Gebruikersinstellingen voor Vingerafdrukken) kunt u instellingen opgeven die het uiterlijk en gedrag van de vingerafdrukherkenning bepalen.

▲ Klik op de pagina Fingerprints op **User Settings** (Gebruikersinstellingen) om de gebruikersinstellingen voor de vingerafdrukreferenties te openen.

- **Enable sound feedback** (Geluidsfeedback inschakelen): standaard geeft HP Client Security audio feedback als een vingerafdruk is geveegd, waarbij verschillende geluiden klinken voor specifieke gebeurtenissen. U kunt nieuwe geluiden toewijzen aan deze gebeurtenissen met het tabblad Geluiden in het configuratievenster van Windows, of het selectievakje wissen om de geluidsfeedback uit te schakelen.
- **Show scan quality feedback** (Feedback scankwaliteit weergeven): selecteer dit selectievakje om alls vegen weer te geven, ongeacht de kwaliteit. Wis het selectievakje om alleen vegen met een goede kwaliteit weer te geven.

HP SpareKey - wachtwoord terugzetten

Met HP SpareKey kunt u toegang krijgen tot uw computer (op ondersteunde platforms) door drie beveiligingsvragen te beantwoorden.

HP Client Security vraagt u om uw persoonlijke HP SpareKey in te stellen tijdens de eerste keer instellen in de HP Client Security Setup Wizard.

Uw HP SpareKey instellen:

1. Selecteer op de pagina HP SpareKey van de wizard drie beveiligingsvragen, en voer voor elke vraag een antwoord in.

   U kunt een vraag in een lijst selecteren of zelf een vraag schrijven.

2. Klik of tik op **Enroll** (Registreren).

Uw HP SpareKey verwijderen:

▲ Klik of tik op **Delete your SpareKey** (SpareKey verwijderen).

Nadat uw SpareKey is ingesteld, hebt u toegang tot uw computer met uw SpareKey vanaf een opstartverificatievenster of het welkomstscherm van Windows.

U kunt verschillende vragen kiezen of de antwoorden wijzigen op de pagina SpareKey, die u bereikt vanaf de tegel Password Recovery op de startpagina van HP Client Security.

Om HP SpareKey Settings (instellingen) te openen, waarin een beheerder instellingen kan opgeven voor de HP SpareKey-referentie, klikt u op **Settings** (Instellingen) (beheerdersbevoegdheden vereist).

HP SpareKey Settings

Op de pagina HP SpareKey Settings kunt u instellingen opgeven die het gedrag en gebruik bepalen van de HP SpareKey referentie.

▲ Klik of tik op **Settings** (Instellingen) op de pagina HP SpareKey page om de pagina HP Sparekey Settings te openen (beheerdersbevoegdheden vereist).

Beheerders kunnen de volgende instellingen selecteren:

- Geef de vragen op die elke gebruiker gesteld worden tijdens het instellen van HP SpareKey.
- Voeg tot drie aangepaste beveiligingsvragen toe aan de lijst die de gebruikers wordt gepresenteerd.
- Kies of gebruikers wel of niet hun eigen vragen mogen schrijven.
- Geef op welke verificatieomgevingen (Windows of Opstartverificatie) het gebruik toestaan van HP SpareKey voor het terugzetten van het wachtwoord.

Windows-wachtwoord

HP Client Security maakt het veranderen van uw Windows-wachtwoord gemakkelijker en sneller dan veranderen via het configuratiescherm van Windows.

Zo verandert u het Windows-wachtwoord:

1. Klik of tik op de startpagina van HP Client Security op **Windows Password** (Windows-wachtwoord).
2. Typ het huidige wachtwoord in het tekstvak **Current Windows password** (Huidig Windows-wachtwoord).
3. Typ een nieuw wachtwoord in het tekstvak **New Windows password** (Nieuw Windows-wachtwoord) en typ het nogmaals in het tekstvak **Confirm new password** (Bevestig nieuw wachtwoord).
4. Klik of tik op **Change** (Wijzigen) om het huidige wachtwoord direct te wijzigen naar het nieuwe dat u hebt ingevoerd.

Bluetooth-apparaten

Als de beheerder Bluetooth als verificatiereferentie heeft ingeschakeld, kunt u een Bluetooth-telefoon instellen in samenwerking met andere referenties voor extra beveiliging.

OPMERKING: Alleen Bluetooth-telefoons worden ondersteund.

1. Controleer of Bluetooth op de computer is ingeschakeld en dat de Bluetooth-telefoon in de ontdekkingsstand staat. Om de telefoon te verbinden, moet u mogelijk een automatisch gegenereerde code op het Bluetooth-apparaat typen. Afhankelijk van de configuratie van het Bluetooth-apparaat kan een vergelijking mogelijk zijn van koppelcodes tussen de computer en de telefoon.
2. Om de telefoon te registreren, selecteert u deze en klikt of tikt u op **Enroll** (Registreren).

Om de Bluetooth-apparatinstellingen op pagina 16 pagina te openen waar een beheerder instellingen voor Bluetooth-apparaten kan vastleggen, klikt u op **Settings** (Instellingen) (beheerdersbevoegdheden vereist).

Bluetooth-apparatinstellingen

Beheerders kunnen de volgende instellingen opgeven die het gedrag en het gebruik bepalen van Bluetooth-apparaatreferenties.

Silent Authentication (Stille verificatie)

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity** (Automatisch het verbonden geregistreerde Bluetooth-apparaat gebruiken tijdens

verificatie van uw identiteit): selecteer het selectievakje zodat gebruikers de Bluetooth-referentie kunnen gebruiken voor verificatie zonder dat een handeling van de gebruiker nodig is, of wis het selectievakje om deze optie uit te schakelen.

Bluetooth Proximity (Bluetooth-nabijheid)

- **Lock computer when your enrolled Bluetooth device moves out of range of your computer**-Selecteer het selectievakje om de computer te vergrendelen als een Bluetooth-apparaat dat tijdens het aanmelden gekoppeld was, buiten bereik gaat, of wis het selectievakje om deze optie uit te schakelen.

OPMERKING: De Bluetooth-module van uw computer moet deze mogelijkheid ondersteunen om hiervan gebruik te kunnen maken.

Kaarten

HP Client Security ondersteunt verschillende soorten identificatiekaarten, kleine plastic kaartjes die een computerchip bevatten. Deze omvatten smartcards, contactloze kaarten en nabijheidskaarten. Als een van deze kaarten en de bijbehorende kaartlezer met de computer is verbonden, als de beheerder het bijbehorende stuurprogramma van de fabrikant heeft geïnstalleerd, en als de beheerdeer de kaart heeft geactiveerd als verificatiereferentie, kunt u de kaart gebruiken als verificatiereferentie.

Voor smartcards moet de fabrikant hulpmiddelen leveren om een beveiligingscertificaat en PIN-beheer te installeren die HP Client Security gebruikt in het beveiligingsalgoritme. Het aantal en soort tekens dat als pincode gebruikt wordt, kan verschillen. Een beheerder moet de smartcard initialiseren voordat deze gebruikt kan worden.

De volgende indelingen voor smartcards worden ondersteund door HP Client Security:

- CSP
- PKCS11

De volgende soorten contactloze kaarten worden ondersteund door HP Client Security:

- Contactloze geheugenkaarten HID iCLASS
- Contactloze Classic 1k, 4k, en mini geheugenkaarten

De volgende nabijheidskaarten worden ondersteund door HP Client Security:

- HID Proximity Cards

Zo registreert u een smartcard:

1. Steek de kaart in een aangesloten smartcardlezer.
2. Als de kaart herkend wordt, voert u de pincode van de kaart in en klikt of tikt u op **Enroll** (Registreren).

Zo wijzigt u de pincode van een smartcard:

1. Steek de kaart in een aangesloten smartcardlezer.
2. Als de kaart herkend wordt, voert u de pincode van de kaart in en klikt of tikt u op **Authenticate** (Verifiëren).
3. Klik of tik op **Change PIN** (Pincode wijzigen) en voer de nieuwe pincode in.

Een contactloze of nabijheidskaart registreren:

1. Plaats de kaart op of vlakbij de betreffende lezer.
2. Als de kaart herkend wordt, klikt of tikt u op **Enroll** (Registreren).

Een geregistreerde kaart verwijderen:

1. Bied de kaart aan de lezer aan.
2. Alleen voor smartcards: voer de toegewezen pincode in en klik of tik op **Authenticate** (Verifiëren).
3. Klik of tik op **Delete** (Verwijderen).

Nadat de kaart geregistreerd is, worden details over de kaart weergegeven onder **Enrolled Cards** (Geregistreerde kaarten). Nadat een kaart is verwijderd, wordt deze uit de lijst verwijderd.

voor het gebruik van instellingen voor nabijheids-, contactloze en smartcards waar beheerders instellingen kunnen vastleggen met betrekking tot kaartreferenties, klikt of tikt u op **Settings** (Instellingen) (beheerdersbevoegdheden vereist).

Instellingen voor nabijheids-, contactloze en smartcards

Om instellingen voor een kaart te openen, klikt of tikt u op de kaart in de lijst en vervolgens op de pijl die verschijnt.

Zo wijzigt u de pincode van een smartcard:

1. Bied de kaart aan de lezer aan
2. Voer de toegewezen pincode in en klik of tik op **Continue** (Doorgaan).
3. Voer de nieuwe pincode in en bevestig deze, en klik of tik op **Continue** (Doorgaan).

Zo initialiseert u de pincode van een smartcard:

1. Bied de kaart aan de lezer aan
2. Voer de toegewezen pincode in en klik of tik op **Continue** (Doorgaan).
3. Voer de nieuwe pincode in en bevestig deze, en klik of tik op **Continue** (Doorgaan).
4. Klik of tik op **Ja** om de initialisatie te bevestigen.

Kaartgegevens wissen:

1. Bied de kaart aan de lezer aan
2. Voer de toegewezen pincode van de kaart in (alleen voor smartcards) en klik of tik op **Continue** (Doorgaan).
3. Klik of tik op **Ja** om het verwijderen te bevestigen.

Pincode

Als de beheerder een pincode als verificatiereferentie heeft ingeschakeld, kunt u een pincode instellen in samenwerking met andere referenties voor extra beveiliging.

Zo stelt u een nieuwe pincode in:

- voer de pincode in, voer deze nogmaals in ter bevestiging, en klik of tik op **Apply** (Toepassen).

Ga als volgt te werk om een pincode te verwijderen:

▲ Klik of tik op **Delete** (Verwijderen) en klik of tik ter bevestiging op **Ja**.

voor het gebruik van PIN-Instellingen waar beheerders instellingen kunnen vastleggen met betrekking tot pincode-referenties, klikt of tikt u op **Settings** (Instellingen) (beheerdersbevoegdheden vereist).

Instellingen voor pincode

Op de pagina PIN Settings (Instellingen voor pincode) kunt u de minimale en maximale lengte voor de pincodereferentie opgeven.

RSA SecurID

Als de beheerder RSA heeft ingesteld als verificatiereferentie, en aan de volgende voorwaarden is voldaan, kunt u een RSA SecurID-referentie registreren of verwijderen.

OPMERKING: De juiste instellingen zijn vereist.

- De gebruiker moet zijn gemaakt op een RSA-server.
- De RSA SecurID token toegewezen aan de gebruiker en de computer moeten zijn gekoppeld aan het RSA serverdomein.
- SecurID software is op de computer geïnstalleerd.
- Een verbinding is beschikbaar voor de correct ingestelde RSA-server.

Een RSA SecurID referentie registreren:

▲ Voer uw RSA SecurID gebruikersnaam en passcode in (RSA SecurID Token code of pincode +Token code, afhankelijk van uw omgeving) en klik of tik op **Apply** (Toepassen).

Na een geslaagde registratie verschijnt een bericht "Your RSA SecurID credential has been successfully enrolled" (Uw RSA SecurID referentie is geregistreerd) en de verwijderknop wordt actief.

Een RSA SecurID referentie verwijderen:

▲ Klik op **Delete** (Verwijderen) en klik op **Ja** in het dialoogvenster met de vraag “Are you sure you want to delete your RSA SecurID credential?” (Weet u zeker dat u de RSA SecurID referentie wilt verwijderen?).

Password Manager

Aanmelden bij websites en applicaties gaat gemakkelijker en veiliger als u Password Manager gebruikt. U kunt sterkere wachtwoorden maken die u niet hoeft op te schrijven of te onthouden, en eenvoudig en snel aanmelden met een vingerafdruk, smartcard, nabijheidskaart, contactloze kaart, Bluetooth-telefoon, pincode, RSA-referentie, of uw Windows-wachtwoord.

OPMERKING: Als gevolg van de voortdurend veranderende structuur van Web-aanmeldvensters is het mogelijk dat Password Manager niet voortdurend alle websites ondersteunt.

Password Manager biedt de volgende opties:

Pagina Password Manager

- Klik of tik op een account om automatisch een webpagina of applicatie te starten en aan te melden.
- Gebruik categoriën om uw accounts te organiseren.

Wachtwoordsterkte

- Bekijk of een van uw wachtwoorden een veiligheidsrisico oplevert.
- Bij het toevoegen van aanmeldgegevens moet u de sterkte controleren van individuele wachtwoorden die voor websites en applicaties gebruikt worden.
- De wachtwoordsterkte wordt aangegeven met rode, gele of groene statusindicatoren.

Het pictogram **Password Manager** wordt weergegeven in de linker bovenhoek van het aanmeldvenster voor een webpagina of applicatie. Als voor een website of applicatie geen aanmelding is ingesteld, verschijnt een plusteken op het pictogram.

▲ Klik of tik op het pictogram **Password Manager** om een contextmenu te openen waarin u kunt kiezen uit de volgende opties:

- Add [somedomain.com] to Password Manager ([eendomein.com] toevoegen aan Password Manager
- Open Password Manager (Password Manager openen)
- Icon Settings (Pictograminstellingen)
- Help

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

De volgende opties worden weergegeven in het contextmenu:

- **Add [somedomain.com] to the Password Manager ([eendomein.com] toevoegen aan Password Manager**: hiermee kunt u een aanmelding maken voor het huidige aanmeldscherm.
- **Open Password Manager** (Password Manager openen): start Password Manager.
- **Icon Settings** (Pictograminstellingen): hiermee kunt u voorwaarden opgeven waaronder het pictogram voor **Password Manager** wordt weergegeven.
- **Help**: geeft de HP Client Security Help weer.

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

De volgende opties worden weergegeven in het contextmenu:

- **Fill in logon data** (Aanmeldgegevens invullen): opent een pagina **Verify your identity** (Uw identiteit verifiëren). Als u geverifieerd bent, worden uw aanmeldgegevens in de aanmeldvelden geplaatst, waarna de pagina wordt verzonden (als verzenden is opgegeven bij het maken of bij de laatste bewerking van de aanmelding).
- **Edit Logon** (Aanmelden bewerken): hiermee kunt u uw aanmeldgegevens voor deze website bewerken.
- **Add Logon** (Aanmdelding toevoegen): hiermee kunt u een account toevoegen aan to Password Manager.
- **Open Password Manager** (Password Manager openen): start Password Manager.
- **Help**: geeft de HP Client Security Help weer.

OPMERKING: De beheerder van deze computer heeft mogelijk HP Client Security ingesteld voor het vereisen van meer dan een referentie bij het verifiëren van uw identiteit.

Aanmelingen toevoegen

U kunt eenvoudig een aanmelding toevoegen voor een website of programma door de aanmeldinformatie eenmalig in te voeren. Daarna voert Password Manager automatisch de informatie voor u in. U kunt deze aanmeldingen gebruiken nadat u naar een website of programma bent gegaan.

Een aanmelding toevoegen:

1. Open het aanmeldvenster voor een website of programma.
2. Klik of tik op het pictogram **Password Manager** en klik of tik vervolgens op een van de volgende, afhankelijk of het aanmeldvenster voor een website of een programma is bedoeld:
   - Klik of tik voor een website op **Add [domain name] to Password Manager** ([domeinnaam] toevoegen aan Password Manager).
   - Klik of tik voor een programma op **Add this logon screen to Password Manager** (Dit aanmeldvenster toevoegen aan Password Manager).
3. Voer de aanmeldgegevens in. Aanmeldvelden op het scherm en de bijbehorende velden in het dialoogvenster zijn gemarkeeerd met een vette oranje rand.
   a. Om een aanmeldveld te vullen met een van de vooraf opgemaakte keuzen, klikt of tikt u op de pijlen rechts van het veld.
   b. Klik of tik op **Show password** (Wachtwoord weergeven) om het wachtwoord voor deze aanmelding weer te geven.
   c. Om de aanmeldvelden te laten invullen, maar niet automatisch, wist u het selectievakje **Automatically submit logon data** (Automatisch aanmeldgegevens verzenden).
   d. Klik of tik op **OK** om de verificatiemethode te selecteren die u wilt gebruiken (vingerafdrukken, smartcard, nabijheidskaart, contactloze kaart, Bluetooth-telefon, pincode of wachtwoord) en meld u vervolgens aan met de geselecteerde verificatiemethode.

      Het plusteken verdwijnt van het pictogram voor **Password Manager** om aan te geven dat de aanmelding gemaakt is.
   e. Als Password Manager de aanmeldvelden niet herkent, klikt of tikt u op **More fields** (Meer velden).
      - Selecteer het selectievakje voor elk veld dat vereist is voor aanmelden, of wis het selectievakje voor alle velden die niet vereist zijn voor aanmelden.
      - Klik of tik op **Close** (Sluiten).

Telkens wanneer u naar die website gaat of dat programma opent, verschijnt het pictogram voor **Password Manager** in de linker bovenhoek van het aanmeldvenster voor een website of applicatie om aan te geven dat u uw geregistreerde referentie kunt gebruiken voor aanmelding.

Aanmeldingen bewerken

Zo bewerkt u een aanmelding:

1. Open het aanmeldvenster voor een website of programma.
2. Klik of tik op het pictogram voor **Password Manager** om een dialoogvenster te openen waarin u de aanmeldinformatie kunt bewerken, en klik of tik op **Edit Logon** (Aanmelding bewerken).

   Aanmeldvelden op het scherm en de bijbehorende velden in het dialoogvenster zijn gemarkeeerd met een vette oranje rand.

   U kunt ook accountgegevens bewerken vanaf de pagina Password Manager door op de aanmelding te klikken of tikken om de bewerkopties weer te geven, en vervolgens **Edit** (Bewerken) te selecteren.
3. Bewerk uw aanmeldinformatie.
   - Om de **Account name** (Accountnaam) te bewerken, typt u een nieuwe naam in het veld.
   - Om de naam van een **Category** (Categorie) toe te voegen of te bewerken, voert u de naam in of bewerkt u deze in het veld **Category** (Categorie).
   - Om een **Username** (Gebruikersnaam) aanmeldveld te selecteren met een van de vooraf opgemaakte keuzen, klikt of tikt u op de pijl rechts van het veld.

     Vooraf opgemaakte keuzen zijn alleen beschikbaar bij het bewerken van de aanmelding vanaf de opdracht Edit (Bewerken) in het contextmenu van het pictogram Password Manager.
   - Om een **Password** (Wachtwoord) aanmeldveld te selecteren met een van de vooraf opgemaakte keuzen, klikt of tikt u op de pijl omlaag rechts van het veld.

     Vooraf opgemaakte keuzen zijn alleen beschikbaar bij het bewerken van de aanmelding vanaf de opdracht Edit (Bewerken) in het contextmenu van het pictogram Password Manager.
   - Om extra velden van het venster toe te voegen aan uw aanmelding, klikt of tikt u op **More fields** (Meer velden).
   - Klik of tik op het pictogram **Show password** (Wachtwoord weergeven) om het wachtwoord voor deze aanmelding weer te geven.
   - Om de aanmeldvelden te laten invullen, maar niet automatisch, wist u het selectievakje **Automatically submit logon data** (Automatisch aanmeldgegevens verzenden).
   - Om te markeren dat deze aanmelding een gecompromitteerd wachtwoord bevat, selecteert u het selectievakje **This password is compromised** (Dit wachtwoord is gecompromitteerd).

     Nadat de wijzigingen zijn opgeslagen, worden alle andere aanmeldingen die hetzelfde wachtwoord gebruiken, eveneeens gemarkeerd als gecompromitteerd. Daarna kunt u elke betroffen account bezoeken en de wachtwoorden wijzigen als dat nodig is.
4. Klik of tik op **OK**.

Het menu Quick Links (Snelkoppelingen) van Password Manager gebruiken

Password Manager biedt een snelle en eenvoudige manier om de websites en programma's te starten waarvoor u aanmeldingen hebt gemaakt. Dubbelklik of tubbeltik op de aanmelding voor een website of programma in het menu **Password Manager Quick Links** of vanaf de pagina Password

Manager in HP Client Security, om het aanmeldvenster te openen en de aanmeldgegevens in te vullen.

Als u een aanmelding maakt, wordt deze automatisch toegevoegd aan Password Manager-menu **Quick Links**.

Het menu **Quick Links** weergeven:

- ▲ Druk op de hotkeycombinatie voor **Password Manager** (Ctrl+Windows-toets+h is de fabrieksinstelling). Klik om de sneltoets te wijzigen op de startpagina van HP Client Security op **Password Manager** en klik of tik vervolgens op **Settings** (Instellingen).

Aanmeldingen in categorieën organiseren

Maak een of meer categorieën om de aanmeldingen te ordenen.

Een aanmelding aan een categorie toewijzen:

1. Klik of tik op de startpagina van HP Client Security op **Password Manager**.
2. Klik of tik op een account en klik of tik op **Edit** (Bewerken).
3. Voer een naam in voor een categorie in het veld **Category** (Categorie).
4. Klik of tik op **Opslaan**.

Een account verwijderen uit een categorie:

1. Klik of tik op de startpagina van HP Client Security op **Password Manager**.
2. Klik of tik op een account en klik of tik op **Edit** (Bewerken).
3. Wis de naam van een categorie in het veld **Category** (Categorie).
4. Klik of tik op **Opslaan**.

Een categorie hernoemen:

1. Klik of tik op de startpagina van HP Client Security op **Password Manager**.
2. Klik of tik op een account en klik of tik op **Edit** (Bewerken).
3. Wijzig de naam van een categorie in het veld **Category** (Categorie).
4. Klik of tik op **Opslaan**.

Uw aanmeldingen beheren

Met Password Manager is het eenvoudig om uw aanmeldinformatie vanaf een centrale locatie te beheren, voor gebruikersnamen, wachtwoorden en meerdere aanmeldaccounts.

Uw aanmeldingen staan op de pagina Password Manager.

Uw aanmeldingen beheren:

1. Klik of tik op de startpagina van HP Client Security op **Password Manager**.
2. Klik of tik op een bestaande aanmelding en selecteer een van de volgende opties en volg de instructies op het scherm.
   - **Edit** (Bewerken): bewerk een aanmelding. Zie Aanmeldingen bewerken op pagina 22 voor meer informatie.
   - **Log in** (Aanmelden): meld u aan bij de geselecteerde account.
   - **Delete** (Verwijderen): verwijder de aanmelding voor de geselecteerde account.

Een extra aanmelding toevoegen voor een website of programma:

1. Open het aanmeldvenster voor de website of het programma.
2. Klik of tik op het pictogram voor **Password Manager** om het contextmenu weer te geven.
3. Klik of tik op **Add Logon** (Aanmelding toevoegen) en volg de instructies op het scherm.

De wachtwoordsterkte beoordelen:

Het gebruik van sterke wachtwoorden voor aanmelding bij uw websites en programma's is een belangrijk aspect van het beveiligen van uw identiteit.

Password Manager maakt het bewaken en verbeteren van uw beveiliging gemakkelijk met directe en geautomatiseerede analyses van de sterkte van elk wachtwoord dat gebruikt wordt bij aanmelding voor websites en programma's.

Terwijl u een wachtwoord invoert bij het maken van een aanmelding voor een account in Password Manager, verschijnt een gekleurde balk onder het wachtwoord om de sterkte van het wachtwoord aan te geven. De kleuren geven de volgende waarden aan:

- **Rood**: zwak
- **Geel**: redelijk
- **Groen**: sterk

Instellingen voor het pictogram van Password Manager

Password Manager probeert aanmeldvensters voor websites en programma's te identificeren. Zodra het een aanmeldvenster ziet waarvoor u geen aanmelding hebt gemaakt, vraagt Password u om een

aanmelding voor het venster toe te voegen door het pictogram voor **Password Manager** met een plusteken weer te geven.

1. Klik of tik op het pictogram en klik of tik vervolgens op **Icon Settings** (Pictograminstellingen) om aan te passen hoe Password Manager omgaat met mogelijke aanmeldsites.
   - **Prompt to add logons for logon screens** (Vragen om aanmeldingen toe te voegen voor aanmeldvensters): klik of tik op deze optie om Password Manager u de vraag te laten stellen als een aanmeldvenster verschijnt waarvoor geen aanmelding is ingesteld.
   - **Exclude this screen** (Dit venster uitsluiten): selecteer het selectievakje zodat Password Manager u niet nogmaals vraagt om een aanmelding toe te voegen voor dit aanmeldvenster.
   - **Do not prompt to add logons for logon screens** (Niet vragen om aanmeldingen toe te voegen voor aanmeldvensters): selecteer het keuzerondje.
2. Een aanmelding toevoegen voor een venster dat tot dan toe was uitgesloten:
   a. Meld u aan bij de eerder uitgesloten website.
   b. Om Password Manager het wachtwoord voor deze site te laten onthouden, klikt of tikt u op **Remember** In het pop-upvenster om het wachtwoord op te slaan en een aanmelding voor het scherm te maken.
3. Om extra instellingen voor Password Manager te openen, klikt of tikt u op het pictogram voor Password Manager; klik of tik op **Open Password Manager** (Password Manager openen) en klik of tik op **Settings** (Instellingen) op de pagina Password Manager.

Aanmeldingen importeren en exporteren

Op de pagina Import and Export (Importeren en exporteren) van Password Manager kunt u aanmeldingen importeren die op uw computer zijn opgeslagen door webbrowsers. U kunt tevens gegevens importeren uit een back-upbestand van HP Client Security en gegevens exporteren naar een back-upbestand van HP Client Security.

▲ Om de pagina Import and export te openen, klikt of tikt u op **Import and export** (Importeren en exporteren) op de pagina Password Manager.

Wachtwoorden importeren uit een browser:

1. Klik of tik op de browser van waaruit u wachtwoorden wilt importeren (alleen geïnstalleerde browsers worden weergegeven).
2. Wis het selectievakje vor alle accounts waarvoor u geen wachtwoorden wilt importeren.
3. Klik of tik op **Importeren**.

U kunt gegevens importeren uit of exporteren naar een back-upbestand van HP Client Security via de bijbehorende koppelingen (onder **Other Options** (Andere opties)) op de pagina Import and export.

OPMERKING: Deze functie importeert en exporteert uitsluitend gegevens van Password Manager. Zie Back-ups van gegevens maken en deze herstellen op pagina 29 voor informatie over het maken van back-ups en het herstellen van extra gegevens van HP Client Security.

Gegevens importeren uit een back-upbestand van HP Client Security:

1. Klik of tik op de pagina Import and Export van HP Password Manager op **Import data from an HP Client Security backup file** (Gegevens importeren uit een back-upbestand van HP Client Security).
2. Verifieer uw identiteit.

3. Selecteer het eerder gemaakte back-upbestand of typ het pad in het daarvoor bestemde veld, en klik of tik op **Browse** (Bladeren).
4. Typ het wachtwoord voor de beveiliging van het bestand dn klik of tik op **Volgende**.
5. Klik of tik op **Restore** (Herstellen).

Gegevens exporteren naar een back-upbestand van HP Client Security:

1. Klik of tik op de pagina Import and Export van HP Password Manager op **Export data to an HP Client Security backup file** (Gegevens exporteren naar een back-upbestand van HP Client Security).
2. Verifieer uw identiteit en klik of tik op **Volgende**.
3. Typ een naam voor het back-upbestand. Standaard wordt het bestand opgeslagen in de map Documenten. Om een andere locatie op te geven, klikt of tikt u op **Browse** (Bladeren).
4. Typ en bevestig het wachtwoord voor de beveiliging van het bestand en klik of tik op **Volgende**.

Instellingen

U kunt instellingen opgeven om Password Manager aan te passen.

- **Prompt to add logons for logon screens** (Vraag voor toevoegen van aanmeldingen voor aanmeldvensters): het pictogram voor **Password Manager** met een plusteken verschijnt zodra een aanmeldvenster voor een website of programma is gevonden, wat betekent dat u een aanmelding voor dit venster kunt toevoegen aan het menu **Logons** (Aanmeldingen).

  Om deze functie uit te schakelen, wist u het selectievakje naast **Prompt to add logons for logon screens** (Vraag voor toevoegen van aanmeldingen voor aanmeldvensters).

- **Open Wachtwoord Manager met Ctrl+Win+h**: De standaard hotkey waarmee het menu **Password Manager Quick Links** opent, is Ctrl+Windows-toets+h.

  Tik op deze optie om de sneltoets te wijzigen en voer een nieuwe toetscombinatie in. Combinaties kunnen een of meer van de volgende elementen bevatten: Ctrl, alt, of shiften elke alfabetische of numerieke toets.

  Combinaties die gereserveerd zijn voor Windows of Windows-applicaties kunnen niet worden gebruikt.

- Klik of tik op **Restore defaults** (Standaardwaarden herstellen) om de standaard fabriekswaarden te herstellen.

Geavanceerde instellingen

Beheerders kunnen beveiliging voorafgaand aan opstarten in- of uitschakelen door op het **tandwiel**pictogram (instellingen) in het beginscherm van HP Client Security te klikken.

- **Administrator Policies** (Beleid voor beheerders): hier kunt u aanmeld- en sessiebeleiden voor beheerders instellen.
- **Standard User Policies** (Standaardbeleid voor gebruikers): hier kunt u aanmeld- en sessiebeleiden voor standaardgebruikers instellen.
- **Security Features** (Beveiligingsvoorzieningen): hier kunt u de beveiliging van de computer verbeteren door uw Windows-account te beschermen met sterke verificatie en/of door verificatie voorafgaand aan het starten van Windows in te schakelen.
- **Users** (Gebruikers): Hiermee kunt u gebruikers en hun referenties beheren.

- **My Policies** (Mijn beleiden): hier kunt u uw verificatiebeleiden en registratiestatus bekijken.
- **Backup and Restore** (Back-up en herstellen): hier kunt u een back-up maken van gegevens van HP Client Security of deze herstellen.
- **About HP Client Security** (Over HP Client Security): toont versie-informatie over HP Client Security.

Beleid voor beheerders

U kunt beleid instellen voor aanmelding en sessies voor beheerders van deze computer. Hier ingestelde aanmeldbeleiden bepalen de referenties die een lokale beheerder nodig heeft om zich bij Windows aan te melden. Hier ingestelde sessiebeleiden bepalen de referenties die een lokale beheerder nodig heeft om de identiteit te verifiëren binnen een Windows-sessie.

Standaard worden alle nieuwe of gewijzigde beleiden direct opgelegd na tikken of klikken op **Apply** (Toepassen).

Een nieuw beleid toevoegen:

1. Klik of tik op de startpagina van HP Client Security op het **tandwiel**pictogram .
2. Klik of tik op de pagina Advanced Settings (Geavanceerde instellingen) op **Administrator Policies** (Beleid voor beheerders).
3. Klik of tik op **Add new policy** (Nieuw beleid toevoegen).
4. Klik op de pijltjes omlaag om primaire en (optioneel) secundaire referenties te selecteren voor het nieuwe beleid en klik of tik vervolgens op **Add** (Toevoegen).
5. Klik op **Toepassen**.

Het opleggen van een nieuw of gewijzigd beleid uitstellen:

1. Klik of tik op **Enforce this policy immediately** (Dit beleid direct opleggen).
2. Selecteer **Enforce this policy on the specific date** (Dit beleid op de opgegeven datum opleggen).
3. Voer een datum in of gebruik de pop-upkalender om de datum te selecteren waarop dit beleid moet worden opgelegd.
4. Selecteer eventueel wanneer gebruikers aan het nieuwe beleid herinnerd moeten worden.
5. Klik op **Toepassen**.

Beleiden voor standaardgebruikers

U kunt beleid instellen voor aanmelding en sessies voor standaardgebruikers van deze computer. Hier ingestelde aanmeldbeleiden bepalen de referenties die een standaardgebruiker nodig heeft om zich bij Windows aan te melden. Hier ingestelde sessiebeleiden bepalen de referenties die een standaardgebruiker nodig heeft om de identiteit te verifiëren binnen een Windows-sessie.

Standaard worden alle nieuwe of gewijzigde beleiden direct opgelegd na tikken of klikken op **Apply** (Toepassen).

Een nieuw beleid toevoegen:

1. Klik of tik op de startpagina van HP Client Security op het **tandwiel**pictogram .
2. Klik of tik op de pagina Advanced Settings (Geavanceerde instellingen) op **Standard User Policies** (Beleid voor standaardgebruikers).

3. Klik of tik op **Add new policy** (Nieuw beleid toevoegen).
4. Klik op de pijltjes omlaag om primaire en (optioneel) secundaire referenties te selecteren voor het nieuwe beleid en klik of tik vervolgens op **Add** (Toevoegen).
5. Klik op **Toepassen**.

Het opleggen van een nieuw of gewijzigd beleid uitstellen:

1. Klik of tik op **Enforce this policy immediately** (Dit beleid direct opleggen).
2. Selecteer **Enforce this policy on the specific date** (Dit beleid op de opgegeven datum opleggen).
3. Voer een datum in of gebruik de pop-upkalender om de datum te selecteren waarop dit beleid moet worden opgelegd.
4. Selecteer eventueel wanneer gebruikers aan het nieuwe beleid herinnerd moeten worden.
5. Klik op **Toepassen**.

Beveiligingfuncties

U kunt voorzieningen voor HP Client Security inschakelen die helpen beschermen tegen ongeoorloofde toegang tot de computer.

Beveiligingsvoorzieningen instellen:

1. Klik of tik op de startpagina van HP Client Security op het **tandwiel**pictogram .
2. Klik of tik op de pagina Advanced Settings (Geavanceerde instellingen) op **Security Features** (Beveiligingsvoorzieningen).
3. Schakel beveiligingsvoorzieningen in door de selectievakjes te kieen en op **Apply** (Toepassen) te klikken of tikken. Hoe meer voorzieningen u selecteert, des te beter uw computer beveiligd wordt.

   Deze instellingen zijn van toepassing op alle gebruikers.

   - **Windows Logon Security** (Beveiliging Windows-aanmelding): bechermt uw Windows-accounts door het gebruik te verplichten van beveiligingsreferenties van HP Client Security voor toegang.
   - **Pre-Boot Security** (Power-on authentication) (Beveiliging voorafgaand aan opstarten (Opstartverificatie)): beveiligt de computer voordat Windows start. Deze selectie is niet beschikbaar als het BIOS dit niet ondersteunt.
   - **Allow One Step logon** (Eenmalig aanmelden toestaan): door deze instelling wordt het aanmelden bij Windows overgeslagen als al eerder verificatie is uitgevoerd tijdens de opstartverificatie of op het niveau van Drive Encryption.
4. Klik of tik op **Users** (Gebruikers) en klik of tik vervolgens op de tegel van de gebruiker.

Gebruikers

U kunt de gebruikers van HP Client Security op deze computer bewaken en beheren.

Een andere Windows-gebruiker toevoegen aan HP Client Security:

1. Klik of tik op de startpagina van HP Client Security op het **tandwiel**pictogram .
2. Klik of tik op de pagina Advanced Settings (Geavanceerde instellingen) op **Users** (Gebruikers).

3. Klik of tik op **Add another Windows user to HP Client Security** (Een andere Windows-gebruiker toevoegen aan HP Client Security).
4. Voer de naam in van de gebruiker die u wilt toevoegen en klik of tik op **OK**.
5. Voer het Windows-wachtwoord van de gebruiker in.

   Op de pagina User (Gebruiker) verschijnt een tegel voor de toegevoegde gebruiker.

Een Windows-gebruiker verwijderen uit HP Client Security:

1. Klik of tik op de startpagina van HP Client Security op het **tandwiel**pictogram .
2. Klik of tik op de pagina Advanced Settings (Geavanceerde instellingen) op **Users** (Gebruikers).
3. Klik of tik op de naam van de gebruiker die u wilt verwijderen.
4. Klik of tik op **Delete User** (Gebruiker verwijderen) en klik of tik vervolgens op **Ja** om te bevestigen.

Een overzicht weergeven van aanmeld- en sessiebeleiden die voor een gebruiker zijn opgelegd:

▲ Klik of tik op **Users** (Gebruikers) en klik of tik vervolgens op de tegel van de gebruiker.

Mijn Beleiden

U kunt uw verificatiebeleiden en registratiestatus weergeven. De pagina My Policies (Mijn beleiden) bevat tevens koppelingen naar de pagina's met beleiden voor beheerders en beleiden voor standaardgebruikers.

1. Klik of tik op de startpagina van HP Client Security op het **tandwiel**pictogram .
2. Klik of tik op de pagina Advanced Settings (Geavanceerde instellingen) op **My Policies** (Mijn beleiden).

   Aanmeld- en sessiebeleiden verschijnen die zijn opgelegd voor de aangemelde gebruiker.

De pagina My Policies (Mijn beleiden) bevat ook koppelingen naar Beleid voor beheerders op pagina 27 en Beleiden voor standaardgebruikers op pagina 27.

Back-ups van gegevens maken en deze herstellen

Aanbevolen wordt om de gegevens van HP Client Security regelmatig in een back-up op te slaan. Hoe vaak u een back-up maakt, is afhankelijk van het tempo waarin de gegevens veranderen. Als u bijvoorbeeld dagelijks nieuwe aanmeldingen toevoegt, moet u dagelijks een back-up maken van de gegevens.

Back-ups zijn tevens bruikbaar voor het migreren naar een andere computer, ook importeren en exporteren genoemd.

OPMERKING: Deze functie maakt alleen een back-up van Password Manager. Drive Encryption beschikt over een eigen back-upmethode. Informatie over Device Access Manager en vingerafdrukverificatie wordt niet in de back-up opgenomen.

HP Client Security moet geïnstalleerd zijn op elke computer waarop back-upgegevens geplaatst zullen worden voordat de gegevens hersteld kunnen worden vanuit het back-upbestand.

Ga als volgt te werk om een back-up te maken van uw gegevens:

1. Klik of tik op de startpagina van HP Client Security op het **tandwiel**pictogram .
2. Klik of tik op de pagina Advanced Settings (Geavanceerde instellingen) op **Administrator Policies** (Beleid voor beheerders).
3. Klik of tik op **Backup and Restore** (Back-up en herstellen).
4. Klik of tik op **Backup** (Back-up) en verifieer uw identiteit.
5. Selecteer de module die u in de back-up wilt opnemen en klik of tik op **Volgende**.
6. Typ een naam voor het opslagbestand. Standaard wordt het bestand opgeslagen in de map Documenten. Om een andere locatie op te geven, klikt of tikt u op **Browse** (Bladeren).
7. Typ en bevestig een wachtwoord om het bestand te beveiligen.
8. Klik of tik op **Opslaan**.

Ga als volgt te werk om gegevens te herstellen:

1. Klik of tik op de startpagina van HP Client Security op het **tandwiel** pictogram.
2. Klik of tik op de pagina Advanced Settings (Geavanceerde instellingen) op **Administrator Policies** (Beleid voor beheerders).
3. Klik of tik op **Backup and Restore** (Back-up en herstellen).
4. Selecteer **Restore** (Herstellen) en verifieer uw identiteit.
5. Selecteer het eerder gemaakte back-upbestand. Typ het pad in het daarvoor bestemde veld. Om een andere locatie op te geven, klikt of tikt u op **Browse** (Bladeren).
6. Typ het wachtwoord voor de beveiliging van het bestand dn klik of tik op **Volgende**.
7. Selecteer de modules waarvoor u de gegevens wilt herstellen.
8. Klik of tik op **Restore** (Herstellen).

5 HP Drive Encryption (alleen bepaalde modellen)

HP Drive Encryption levert volledige gegevensbescherming door de gegevens op uw computer te coderen. Als Drive Encryption is ingeschakeld, moet u zich aanmelden op het aanmeldvenster van Drive Encryption, dat verschijnt voordat het besturingssysteem Windows® start.

In het beginscherm van HP Client Security kunnen Windows-beheerders Drive Encryption activeren, een back-up maken van de coderingssleutel, en station(s) of partitie(s) selecteren of deselecteren voor codering. Zie de Help voor de HP Client Security software voor meer informatie.

De volgende taken zijn mogelijk met Drive Encryption:

- Instellingen voor Drive Encryption selecteren:
  - Coderen of decoderen van individuele schijfeenheden of partities met software-codering
  - Coderen of decoderen van individuele zelfcoderende schijfeenheden met hardware-codering
  - Extra beveiliging toevoegen door slaapmodus of stand-by uit te schakelen om er voor te zorgen dat de verificatie voorafgaand aan opstarten van Drive Encryption altijd vereist is.

OPMERKING: Alleen interne SATA en externe eSATA vaste schijven kunnen gecodeerd worden.

- Back-ups maken van sleutels
- Toegang herstellen tot een gecodeerde computer met back-upsleutels en HP SpareKey
- Verificatie voorafgaand aan opstarten van Drive Encryption inschakelen met een wachtwoord, vastgelegde vingerafdruk, of pincode voor geselecteerde smartcards

Drive Encryption openen

Beheerders hebben toegang tot Drive Encryption door HP Client Security te openen:

1. Klik of tik op het startscherm op de app **HP Client Security** (Windows 8).

   – of –

   Dubbelklik of dubbeltik op het bureaublad van Windows op het pictogram **HP Client Security** in het systeemvak, rechts op de taakbalk.

2. Klik of tik op het pictogram **Drive Encryption**.

Algemene taken

Drive Encryption activeren voor standaard vaste schijven

Standaard vaste schijven worden gecodeerd met softwarecodering. Ga als volgt te werk om een schijfeenheid of een schijfpartitie te coderen:

1. Start **Drive Encryption**. Zie Drive Encryption openen op pagina 31 voor meer informatie.
2. Selecteer het selectievakje voor de schijfeenheid of de partitie die u wilt coderen en klik of tik op **Back-upsleutel**.

OPMERKING: Selecteer voor een betere veiligheid het selectievakje **Disable sleep mode for increased security** (Slaapstand uitschakelen voor een betere veiligheid). Als u de slaapstand uitschakelt, bestaat absoluut geen gevaar dat de referenties die gebruikt worden om de schijfeenheid te ontsluiten, in het geheugen worden opgeslagen.

3. Selecteer een of meer back-up opties en klik of tik op **Back-up**. Zie Back-up maken van coderingssleutel op pagina 35 voor meer informatie.
4. U kunt doorgaan met werken terwijl een back-up wordt gemaakt van de coderingssleutel. Herstart de computer niet.

OPMERKING: U wordt gevraagd om de computer te herstarten. Na het herstarten verschijnt het scherm van Drive Encryption dat aan het opstarten vooraf gaat en dat om verificatie vraagt voordat Windows start.

Drive Encryption is geactiveerd. Codering van de geselecteerde schijfpartitie(s) kan een aantal uren duren, afhankelijk van het aantal en de omvang van de partitie(s).

Zie de Help voor de HP Client Security software voor meer informatie.

Drive Encryption activeren voor zelfcoderende schijven

Zelfcoderende schijven die voldoen aan de OPAL-specificatie van de Trusted Computing Group voor het beheer van zelfcoderende schijven, kunnen zowel met software- als hardwarecodering worden gecodeerd. Hardwarecodering verloopt veel sneller dan softwarecodering. Maar u kunt niet kiezen welke schijfpartities gecodeerd worden. De gehele schijf wordt gecodeerd, inclusief eventuele schijfparties.

Om specifieke partities te coderen, hebt u softwarecodering nodig. Wis het selectievakje **Only allow hardware encryption for Self-Encrypting Drives (SEDs)** (Alleen hardwarecodering toestaan voor zelfcoderende schijven (SED's)).

Ga als volgt te werk om Drive Encryption te activeren voor zelfcoderende schijven:

1. Start **Drive Encryption**. Zie Drive Encryption openen op pagina 31 voor meer informatie.
2. Selecteer het selectievakje voor de schijfeenheid die u wilt coderen, en klik of tik op **Back-upsleutel**.

OPMERKING: Selecteer voor een betere veiligheid het selectievakje **Disable sleep mode for added security** (Slaapstand uitschakelen voor een betere veiligheid). Als u de slaapstand uitschakelt, bestaat absoluut geen gevaar dat de referenties die gebruikt worden om de schijfeenheid te ontsluiten, in het geheugen worden opgeslagen.

3. Selecteer een of meer back-up opties en klik of tik op **Back-up**. Zie Back-up maken van coderingssleutel op pagina 35 voor meer informatie.
4. U kunt doorgaan met werken terwijl een back-up wordt gemaakt van de coderingssleutel. Herstart de computer niet.

OPMERKING: Voor zelfcoderende schijfeenheden wordt u gevraagd om de computer af te sluiten.

Zie de Help voor de HP Client Security software voor meer informatie.

Drive Encryption uitschakelen

1. Start **Drive Encryption**. Zie Drive Encryption openen op pagina 31 voor meer informatie.
2. Wis het selectievakje voor alle gecodeerde schijfeenheden en klik of tik op **Toepassen**.

   Het uitschakelen van Drive Encryption begint.

OPMERKING: Als softwarecodering is toegepast, start het decoderen. Het kan een aantal uren duren, afhankelijk van de omvang van de gecodeerde schijfpartitie(s). Na afloop van het decoderen is Drive Encryption uitgeschakeld.

Bij toepassing van hardwarecodering is de schijfeenheid direct gedecodeerd en is Drive Encryption na een paar minuten uitgeschakeld.

Nadat Drive Encryption is uitgeschakeld, wordt u gevraagd om de computer af te sluiten, bij hardwarecodering, of om de computer te herstarten, bij softwarecodering.

Aanmelden nadat Drive Encryption is geactiveerd

Als u de computer inschakelt na het uitschakelen van Drive Encryption en uw gebruikersaccount is geregistreerd, moet u zich aanmelden in het aanmeldvenster van Drive Encryption.

OPMERKING: Bij het ontwaken uit de slaap- of stand-bymodus, wordt verificatie voorafgaand aan opstarten van Drive Encryption niet weeergegeven voor software- of hardwarecodering. Hardwarecodering biedt de optie **Disable sleep mode for increased security** (Slaapmodus uitschakelen voor extra veiligheid) die voorkomt dat de slaap- of stand-bymodus actief wordt als dit is ingeschakeld.

Bij het ontwaken uit de hibernationstand, wordt verificatie voorafgaand aan opstarten van Drive Encryption weeergegeven voor software- of hardwarecodering.

OPMERKING: Als de beheerder van Windows BIOS Pre-boot Security in HP Client Security heeft ingeschakeld en als One-Step Logon is ingeschakeld (standaard), kunt u zich aanmelden bij de computer direct na verificatie bij BIOS Pre-boot, zonder extra verificatie in het aanmeldvenster van Drive Encryption.

Aanmelden enkele gebruiker:

- Voer op de pagina **Aanmelden** uw wachtwoord voor Windows, pincode van smartcard, SpareKey in, of veeg met een vastgelegde vinger.

Aanmelden meerdere gebruikers:

1. Selecteer op de pagina **Select user to logon** (Gebruiker voor aanmelden selecteren) de gebruiker die zich moet aanmelden in de keuzelijst en klik of tik op **Volgende**.
2. Voer op de pagina **Aanmelden** uw wachtwoord voor Windows of pincode van smartcard in, of veeg met een vastgelegde vinger.

OPMERKING: De volgende smartcards worden ondersteund:

Ondersteunde smartcards

- Gemalto Cyberflex Access 64k V2c

OPMERKING: Als de herstelsleutel gebruikt wordt voor aanmelden in het aanmeldvenster voor Drive Encryption, zijn extra referenties nodig bij het aanmelden bij Windows om toegang te krijgen tot gebruikersaccounts.

Extra vaste schijven coderen

Het wordt sterk aangeraden om HP Drive Encryption te gebruiken om uw gegevens te beveiligen, door de vaste schijf te coderen. Na activeren kunt u op de volgende wijze alle vaste schijven of gemaakte partities coderen:

1. Start **Drive Encryption**. Zie Drive Encryption openen op pagina 31 voor meer informatie.
2. Selecteer voor software-gecodeerde schijfeenheden de te coderen schijfpartities.

OPMERKING: Dit is ook van toepassing bij een scenario met gemengde schijfeenheden waarin een of meer standaard vaste schijven en een of meer zelfcoderende schijfeenheden aanwezig zijn.

– of –

▲ Selecteer voor hardware-gecodeerde schijfeenheden de extra te coderen schijfeenheden.

Geavanceerde taken

Drive Encryption beheren (taak voor beheerder)

Beheerders kunnen Drive Encryption gebruiken om de coderingsstatus te bekijken en te wijzigen (Niet gecodeerd of Gecodeerd) van alle vaste schijven in de computer.

- Als de status Ingeschakeld is, is Drive Encryption ingeschakeld en ingesteld. De schijfeenheid bevindt zich in een van de volgende staten:

Softwarecodering

- Niet gecodeerd
- Gecodeerd
- Codering
- Decoderen

Hardwarecodering

- Gecodeerd
- Niet gecodeerd (voor extra schijfeenheden)

Individuele schijfpartities coderen of decoderen (alleen softwarecodering)

Beheerders kunnen Drive Encryption gebruiken om een of meer schijfpartities op de computer te coderen of om schijfpartities te decoderen die reeds gecodeerd zijn.

1. Start **Drive Encryption**. Zie Drive Encryption openen op pagina 31 voor meer informatie.
2. Selecteer of wis onder **Drive Status** (Status schijfeenheid) het selectievakje naast elke vaste schijfpartitie die u wilt coderen of decoderen, en klik of tik op **Toepassen**.

OPMERKING: Tijdens het coderen of decoderen van een partitie geeft een voortgangsbalk het percentage van de partitie aan dat gecodeerd is.

OPMERKING: Dynamische partities worden niet ondersteund. Als een partitie als beschikbaar is weergegeven, maar na selectie niet gecodeerd kan worden, is dat een dynamische partitie. Een dynamische partitie ontstaat als een partitie verkleind is om een nieuwe partitie te maken binnen Schijfbeheer.

Een waarschuwing verschijnt als een partitie wordt omgezet naar een dynamische partitie.

Schijfbeheer

- **Nickname** (Bijnaam): u kunt schijfeenheden en partities namen geven zodat u ze gemakkelijker kunt herkennen.
- **Disconnected drives** (Schijfeenheden ontkoppelen): Drive Encryption kan bijhouden welke schijfeenheden van de computer ontkoppeld zijn. Een schijfeenheid die van de computer is ontkoppeld, wordt automatisch verplaatst naar de lijst Disconnected (Ontkoppeld). Als de schijf weer in het systeem terugkomt, verschijnt hij weer in de lijst Connected (Gekoppeld).
- Als u de ontkoppelde schijfeenheid niet langer hoeft te volgen of beheren, kunt u de ontkoppelde schijf verwijderen uit de lijst Disconnected (Ontkoppeld).
- Drive Encryption blijft ingeschakeld tot de selectievakjes voor alle gekoppelde schijfeenheden gewist zijn en de lijst Disconnected (Ontkoppeld) leeg is.

Back-up en terugzetten (beheerderstaak)

Als Drive Encryption is ingeschakeld, kunnen beheerders de pagina Encryption Key Backup (Back-up van coderingssleutel) gebruiken om back-ups te maken van coderingssleutels op verwisselbare media en om een terugzetactie uit te voeren.

Back-up maken van coderingssleutel

Beheerders kunnen een back-up maken van de coderingssleutel voor een gecodeerde schijfeenheid op een verwisselbaar opslagapparaat.

VOORZICHTIG: Zorg er voor dat het opslagapparaat met de back-upsleutel op een veilige plaats wordt opgeslagen, want als u het wachtwoord vergeet, uw smartcard kwijt raakt of geen vastgelegde vinger hebt, biedt dit apparaat alleen toegang tot de computer. De plaats voor opslag moet eveneens beveiligd zijn, omdat het opslagapparaat toegang tot Windows biedt.

1. Start **Drive Encryption**. Zie Drive Encryption openen op pagina 31 voor meer informatie.
2. Selecteer het selectievakje voor een schijfeenheid en klik of tik op **Backup Key** (Back-upsleutel).

3. Selecteer onder **Create HP Drive Encryption recovery key** (Herstelsleutel voor HP Drive Encryption maken) een of meer van de volgende opties:

   - **Removable Storage** (Verwisselbare opslag): selecteer het selectievakje en vervolgens het opslagapparaat waarop de coderingssleutel wordt opgeslagen.
   - **SkyDrive**: selecteer het selectievakje. U moet met internet verbonden zijn. Meld u aan bij Microsoft SkyDrive en klik of tik op **Ja**.

   OPMERKING: Om de back-upsleutel voor HP Drive Encryption te gebruiken die is opgeslagen op SkyDrive, moet u die downloaden van SkyDrive naar een verwisselbaar opslagapparaat en dit vervolgens in de computer steken.

   - **TPM** (alleen geselecteerde modellen): hiermee kunt u uw gegevens terugzetten met uw wachtwoord voor TPM.

   VOORZICHTIG: Als de TPM gewist is of de computer is beschadigd, hebt u geen toegang meer tot de back-up. Als deze methode is geselecteerd, moet tevens een andere back-upmethode zijn geselecteerd.

4. Klik of tik op **Backup** (Back-up).

   De coderingssleutel wordt opgeslagen op het geselecteerde opslagapparaat.

Toegang herstellen tot een geactiveerde computer met back-upsleutels

Beheerders kunnen een terugzetactie uitvoeren met de sleutel van Drive Encryption waarvan een back-up is gemaakt op een verwisselbaar opslagapparaat tijdens activering of door de optie **Backup Key** (Back-upsleutel) te kiezen in Drive Encryption.

1. Plaats het verwisselbaar opslagapparaat dat de back-upsleutel bevat.
2. Schakel de computer in.
3. Klik of tik als het aanmeldvenster van HP Drive Encryption verschijnt op **Recovery** (Terugzetten).
4. Voer het bestandspad of de bestandsnaam in dat de back-upsleutel bevat en klik of tik op **Recovery** (Terugzetten).
5. Klik of tik als het bevestigingsvenster verschijnt op **OK**.

   Het aanmeldvenster van Windows verschijnt.

OPMERKING: Als de herstelsleutel gebruikt wordt voor aanmelden in het aanmeldvenster voor Drive Encryption, zijn extra referenties nodig bij het aanmelden bij Windows om toegang te krijgen tot gebruikersaccounts. Het wordt sterk aangeraden om het wachtwoord te wijzigen nadat een terugzetactie is uitgevoerd.

Een terugzetactie met HP SpareKey uitvoeren

SpareKey Recovery binnen Drive encryption Pre-boot vereist dat u beveiligingsvragen juist beantwoordt voordat u de computer kunt gebruiken. Zie de Help voor de HP Client Security software voor meer informatie over het opzetten van Sparekey Recovery.

HP SpareKey Recovery uitvoeren als u uw wachtwoord vergeten hebt:

1. Schakel de computer in.
2. Als de pagina HP Drive Encryption wordt weergegeven, navigeert u naar het aanmeldscherm.

3. Klik op **SpareKey**.

OPMERKING: Als uw SpareKey niet is geïnitialiseerd in HP Client Security, is de knop **SpareKey** niet beschikbaar.

4. Typ de juiste antwoorden op de weergegeven vragen en klik vervolgens **Logon** (Aanmelden).

   Het aanmeldvenster van Windows verschijnt.

OPMERKING: Als SpareKey gebruikt wordt voor aanmelden in het aanmeldvenster voor Drive Encryption, zijn extra referenties nodig bij het aanmelden bij Windows om toegang te krijgen tot gebruikersaccounts. Het wordt sterk aangeraden om het wachtwoord te wijzigen nadat een terugzetactie is uitgevoerd.

6 HP File Sanitizer (alleen bepaalde modellen)

Met File Sanitizer kunt u goed veilig apparatuur vernietigen (bijvoorbeeld: persoonlijke informatie of bestanden, historische of Web-gerelateerde gegevens, of andere gegevenscomponenten) op de interne harde schijf van de computer en om regelmatig de interne vaste schijf van de computer schoon te maken.

U kunt File Sanitizer niet gebruiken voor het opruimen of bleken van de volgende soorten schijven:

- Solid-state drives (SSD), inclusief RAID-volumes die een SSD-apparaat omvatten
- Externe schijven aangesloten via USB, Firewire, of eSATA

Als een vernietigings- of schoonmaakoperatie op een SSD wordt gepoogd, verschijnt een waarschuwing en wordt de handeling niet uitgevoerd.

Vernietigen

Vernietigen is niet hetzelfde als standaard verwijderen onder Windows®. Als u een onderdeel vernietigt met File Sanitizer, worden de bestanden overschreven met betekenisloze gegevens, waardoor het vrijwel onmogelijk is om het origineel te herstellen. Een eenvoudige verwijderactie onder Windows laat het bestand intact op de vaste schijf of het blijft in een staat achter waarmee het met forensische methoden hersteld kan worden.

U kunt een tijd voor vernietigen instellen of u kunt vernietigen handmatig activeren door op het pictogram **File Sanitizer** te klikken op het venster HP Client Security Home of met het pictogram **File Sanitizer** op het bureaublad van Windows. Zie voor meer informatie Een vernietigingsschema instellen op pagina 40, Rechtsklikken om te vernietigen op pagina 42 of Handmatig een vernietigingsactie starten op pagina 42.

OPMERKING: Een .dll-bestand wordt alleen vernietigd en van het systeem verwijderd als het naar de prullenmand is verplaatst.

Opschonen van vrije ruimte

Een gegevenselement verwijderen onder Windows verwijdert de inhoud daarvan niet volledig van de vaste schijf. Windows verwijdert alleen de verwijzing naar het gegevenselement, of de locatie op de vaste schijf. De inhoud van het gegevenselement blijft op de schijf achter totdat een ander gegevenselement dat gebied op de schijf overschrijft met nieuwe informatie.

Door vrije ruimte schoon te maken, kunt u veilig willekeurige gegevens over verwijderde gegevenselementen schrijven zodat gebruikers de originele inhoud van de verwijderde gegevenselementen niet meer kunnen bekijken.

OPMERKING: Door vrije ruimte schoon te maken, voegt u geen extra beveliging toe aan verwijderde gegevenselementen.

U kunt een tijd voor bleken plannen of u kunt bleken van vrije ruimte handmatig activeren door op het pictogram **File Sanitizer** te klikken op het venster HP Client Security Home of met het pictogram **File Sanitizer** op het bureaublad van Windows. Zie voor meer informatie Een planning instellen voor het

bleken van vrije ruimte op pagina 41, Handmatig vrije ruimte bleken starten op pagina 43 of Het pictogram File Sanitizer gebruiken op pagina 42.

File Sanitizer openen

1. Klik of tik op het startscherm op de app **HP Client Security** (Windows 8).

   – of –

   Dubbelklik of dubbeltik op het bureaublad van Windows op het pictogram **HP Client Security** in het systeemvak, rechts op de taakbalk.

2. Klik of tik onder **Gegevens** op **File Sanitizer**.

– of –

▲ Dubbelklik of dubbeltik op het pictogram **File Sanitizer** op het bureaublad van Windows.

– of –

▲ Rechtsklik op of houd het pictogram **File Sanitizer** ingedrukt op het bureaublad van Windows en selecteer **File Sanitizer openen**.

Installatieprocedures

Shredding (Vernietiging): File Sanitizer verwijdert of vernietigt op veilige wijze geselecteerde categorieën van gegevenselementen.

1. Selecteer onder **Schredding** (Vernietiging) het selectievakje voor elk type bestand dat u wilt vernietigen, of wis het selectievakje als u dat type bestand niet wilt vernietigen.

   - **Prullenbak**: vernietigt alle items in de prullenbak.
   - **Tijdelijke systeembestanden**: vernietigt alle bestanden in de tijdelijke map van het systeem. De volgende omgevingsvariabelen worden in onderstaande volgorde doorzocht en het eerst gevonden pad wordt als systeemmap beschouwd:
     - TMP
     - TEMP
   - **Tijdelijke internetbestanden**: vernietigt kopieën van webpagina's, afbeeldingen en media die door webbrowsers zijn opgeslagen om de weergave te versnellen.
   - **Cookies**: vernietigt alle bestanden die door websites op een computer zijn opgeslagen om voorkeuren op te slaan, zoals aanmeldgegevens.

2. Klik of tik op **Vernietig** om het vernietigen te starten.

Bleken: schrijft willekeurige gegevens naar vrije ruimte en voorkomt dat verwijderde items hersteld kunnen worden.

▲ Klik of tik op **Bleken** om het schoonmaken te starten.

File Sanitizer Options (Opties File Sanitizer): markeer het selectievakje om elk van de volgende opties in te schakelen, of wis het selectievakje om een optie uit te schakelen:

- **Enable Desktop icon** (Bureaubladpictogram inschakelen): geeft het pictogram van File Sanitizer weer op het bureaublad van Windows.
- **Enable right-click** (Rechtsklikken inschakelen): hiermee kunt u op een gegevenselement rechtsklikken of tikken en het vasthouden, waarna u **HP File Sanitizer – Vernietigen** selecteert.

- **Ask for Windows password before manual shredding** (Naar Windows-wachtwoord vragen voor handmatig vernietigen): vereist verificatie met het wachtwoord van Windows voordat u een item handmatig vernietigt.
- **Shred Cookies and Temporary Internet Files on browser close** (Cookies en tijdelijke internetbestanden vernietigen bij sluiten browser): vernietigt alle geselecteerde op het web betrekking hebbende gegevenselementen, zoals de URL-geschiedenis van de browser, als u een webbrowser sluit.

Een vernietigingsschema instellen

U kunt een tijd plannen om vernietigen automatisch uit te voeren, of u kunt gegevenselementen ook op elk tijdstip met de hand vernietigen. Raadpleeg Installatieprocedures op pagina 39 voor meer informatie.

1. Open File Sanitizer en klik of tik op **Instellingen**.
2. Om een toekomstige tijd te plannen voor het vernietigen van geselecteerde gegevenselementen, selecteert u onder **Shred Schedule** (Planning vernietiging) de optie **Nooit**, **Eenmaal**, **Dagelijks**, **Wekelijks** of **Maandelijks**, waarna u een dag en tijd selecteert:
   a. Klik of tik op het uur, de minuut, of het veld AM/PM.
   b. Blader tot de gewenste waarde op hetzelfde niveau wordt weergegeven als de andere velden.
   c. Klik of tik op de witte ruimte rond de velden voor het instellen van de tijd.
   d. Herhaal dit voor elk veld tot de juiste planning is geselecteerd.
3. De volgende vier typen gegevenselementen zijn opgenomen:
   - **Prullenbak**: vernietigt alle items in de prullenbak.
   - **Tijdelijke systeembestanden**: vernietigt alle bestanden in de tijdelijke map van het systeem. De volgende omgevingsvariabelen worden in onderstaande volgorde doorzocht en het eerst gevonden pad wordt als systeemmap beschouwd:
     - TMP
     - TEMP
   - **Tijdelijke internetbestanden**: vernietigt kopieën van webpagina's, afbeeldingen en media die door webbrowsers zijn opgeslagen om de weergave te versnellen.
   - **Cookies**: vernietigt alle bestanden die door websites op een computer zijn opgeslagen om voorkeuren op te slaan, zoals aanmeldgegevens.

   Als deze gegevenselementen geselecteerd zijn, worden ze op de geplande tijd vernietigd.
4. Zo selecteert u nog meer gegevenselementen om te vernietigen:
   a. Klik of tik onder **Scheduled Shred List** (Geplande vernietigingslijst) op **Map toevoegen** en ga vervolgens naar het bestand of de map.
   b. Klik of tik op **Openen** en klik of tik op **OK**.

   Om een gegevenselement te verwijderen uit de lijst, wist u het selectievakje voor het gegevenselement.

Een planning instellen voor het bleken van vrije ruimte

Door vrije ruimte schoon te maken, voegt u geen extra beveliging toe aan verwijderde gegevenselementen.

1. Open File Sanitizer en klik of tik op **Instellingen**.
2. Om een toekomstige tijd te selecteren voor het schoonmaken van uw vaste schijf, selecteert u onder **Bleach Schedule** (Schoonmaakschema) **Never** (Nooit), **Once** (Eenmaal), **Daily** (Dagelijks), **Weekly** (Wekelijks), of **Monthly** (Maandelijks), en vervolgens een dag en tijd.
   a. Klik of tik op het uur, de minuut, of het veld AM/PM.
   b. Blader tot de gewenste waarde op hetzelfde niveau wordt weergegeven als de andere velden.
   c. Klik of tik op de witte ruimte rond de velden voor het instellen van de tijd.
   d. Herhaal dit tot de juiste planning is geselecteerd.

OPMERKING: Opruimen van vrije ruimte kan veel tijd kosten. Zorg er voor dat uw computer op het lichtnet is aangesloten. Bleken van vrije ruimte wordt weliswaar op de achtergrond uitgevoerd, maar de prestaties van de computer kunnen beïnvloed worden door het toegenomen gebruik van de processor. Opruimen van vrije ruimte kan na werktijd plaatsvinden of als de computer niet in gebruik is.

Bestanden tegen vernietigen beveiligen

Voorkomen dat bestanden of mappen vernietigd worden:

1. Open File Sanitizer en klik of tik op **Instellingen**.
2. Klik of tik onder **Never Shred List** (Lijst nooit vernietigen) op **Map toevoegen** en ga vervolgens naar het bestand of de map.
3. Klik of tik op **Openen** en klik of tik op **OK**.

OPMERKING: Bestanden in deze lijst worden beschermd zolang ze in de lijst blijven staan.

Om een gegevenselement te verwijderen uit de lijst met uitzonderingen, wist u het selectievakje voor het gegevenselement.

Algemene taken

Gebruik File Sanitizer voor het uitvoeren van de volgende taken:

- **Gebruik het pictogram File Sanitizer om het vernietigen te starten**: sleep bestanden naar het pictogram **File Sanitizer** op het bureaublad van Windows. Zie voor details Het pictogram File Sanitizer gebruiken op pagina 42.
- **Handmatig een bepaald of alle geselecteerde gegevenselementen vernietigen**: vernipper op elk gewenst moment items zonder op een geplande tijd te wachten. Zie voor details Rechtsklikken om te vernietigen op pagina 42 of Handmatig een vernietigingsactie starten op pagina 42.

- **Handmatig vrije ruimte bleken activeren**: activeer op elk gewenst moment bleken van vrije ruimte. Zie voor details Handmatig vrije ruimte bleken starten op pagina 43.
- **De logboekbestanden weergeven**: geef de logboekbestanden weer voor vernietigen en het bleken van vrije ruimte, die fouten bevatten van de laatste vernietigings- of bleekactie. Zie voor details De logboekbestanden weergeven op pagina 43.

OPMERKING: Vernietigen of opruimen van vrije ruimte kan veel tijd kosten. Vernietigen en vrije ruimte bleken worden weliswaar op de achtergrond uitgevoerd, maar de prestaties van de computer kunnen beïnvloed worden door het toegenomen gebruik van de processor.

Het pictogram File Sanitizer gebruiken

VOORZICHTIG: Gegevenselementen die zijn versnipperd, kunnen niet worden hersteld. Bepaal zorgvuldig welke items u voor handmatig vernietigen selecteert.

Als u handmatig een vernietigingsactie start, wordt de standaard vernietigingslijst in de weergave File Sanitizer vernietigd (zie Installatieprocedures op pagina 39).

U kunt op een van de volgende manieren een vernietigingsactie handmatig starten:

1. Open File Sanitizer (zie File Sanitizer openen op pagina 39) en klik of tik op **Schred**.
2. Als het bevestigingsvenster verschijnt, moet u controleren of de gewenste gegevenselementen geselecteerd zijn, waarna u op **OK** klikt of tikt.

– of –

1. Rechtsklik op of houd het pictogram **File Sanitizer** ingedrukt op het bureaublad van Windows en selecteer **Nu vernietigen**.
2. Als het bevestigingsvenster verschijnt, moet u controleren of de gewenste gegevenselementen geselecteerd zijn, waarna u op **Vernietigen** klikt of tikt.

Rechtsklikken om te vernietigen

VOORZICHTIG: Gegevenselementen die zijn versnipperd, kunnen niet worden hersteld. Bepaal zorgvuldig welke items u voor handmatig vernietigen selecteert.

Als **Enable right-click shredding** (Vernietigen met rechtsklikken) is geselecteerd in de weergave File Sanitizer, kunt u een gegevenselement op de volgende manier vernietigen:

1. Navigeer naar het document of de map die u wilt vernietigen.
2. Rechtsklik of tik en houd het bestand of de map vast, en seelcteer vervolgens **HP File Sanitizer – Vernietigen**.

Handmatig een vernietigingsactie starten

VOORZICHTIG: Gegevenselementen die zijn versnipperd, kunnen niet worden hersteld. Bepaal zorgvuldig welke items u voor handmatig vernietigen selecteert.

Als u handmatig een vernietigingsactie start, wordt de standaard vernietigingslijst in de weergave File Sanitizer vernietigd (zie Installatieprocedures op pagina 39).

U kunt op een van de volgende manieren een vernietigingsactie handmatig starten:

1. Open File Sanitizer (zie File Sanitizer openen op pagina 39) en klik of tik op **Schred**.
2. Als het bevestigingsvenster verschijnt, moet u controleren of de gewenste gegevenselementen geselecteerd zijn, waarna u op **OK** klikt of tikt.

– of –

1. Rechtsklik op of houd het pictogram **File Sanitizer** ingedrukt op het bureaublad van Windows en selecteer **Nu vernietigen**.
2. Als het bevestigingsvenster verschijnt, moet u controleren of de gewenste gegevenselementen geselecteerd zijn, waarna u op **Vernietigen** klikt of tikt.

Handmatig vrije ruimte bleken starten

Als u handmatig een opruimactie start, wordt de standaard vernietigingslijst in de weergave File Sanitizer opgeruimd (zie Installatieprocedures op pagina 39).

U kunt op een van de volgende manieren een opruimactie handmatig starten:

1. Open File Sanitizer (zie File Sanitizer openen op pagina 39) en klik of tik op **Bleach**.
2. Klik of tik als het bevestigingsvenster verschijnt op **OK**.

– of –

1. Rechtsklik op of houd het pictogram **File Sanitizer** ingedrukt op het bureaublad van Windows en selecteer **Nu bleken**.
2. Klik of tik als het bevestigingsvenster verschijnt op **Bleken**.

De logboekbestanden weergeven

Telkens wanneer een vernietigings- of opruimactie is uitgevoerd, worden logboekbestanden gegenereerd met fouten. De logboekbestanden worden altijd bijgewerkt aan de hand van de laatste vernietigings- of opruimactie.

OPMERKING: Bestanden waarvan het vernietigen of opruimen geslaagd is, verschijnen niet in de logboekbestanden.

Een logboekbestand wordt gemaakt voor vernietigen en een ander logboekbestand voor opruimen van vrije ruimte Beide logboekbestanden bevinden zich op de harde schijf in de volgende mappen:

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

Op 64-bitssystemen bevinden de logboekbestanden zich op de harde schijf in de volgende mappen:

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

7 HP Device Access Manager (alleen bepaalde modellen)

HP Device Access Manager beheert de toegang tot gegevens door apparaten voor gegevensoverdracht uit te schakelen.

OPMERKING: Van sommige menselijke interface/invoerapparaten, zoals muis, toetsenbord, Touchpad en vingerafdruklezer, wordt de toegang niet beheerd door Device Acces Manager. Zie Onbeheerde apparaatklassen op pagina 48 voor meer informatie.

Beheerders voor het Windows® besturingssysteem gebruiken HP Device Access Manager voor het regelen van toegang tot de apparaten in een systeem en ter bescherming tegen ongeoorloofde toegang:

- Apparaatprofielen worden voor iedere gebruiker gemaakt, om te bepalen tot welke apparaten zij wel of geen toegang hebben.
- Just In Time Authentication (JITA) stelt vooraf gedefinieerde gebruikers in staat om zich zelf te verifiëren om apparaten te benaderen waarvoor de toegang anders wordt geweigerd.
- Beheerders en vertrouwde gebruikers kunnen worden uitgesloten van de beperkingen op de toegang tot apparaten door Device Access Manager door ze toe te voegen aan de groep apparaatbeheerders. Het lidmaatschap voor deze groep wordt beheerd met Geavanceerde instellingen.
- Apparaattoegang kan worden verleend of geweigerd op basis van het groepslidmaatschap of voor individuele gebruikers.
- Voor apparaatklassen zoals cd-romstations en dvd-stations, kunnen leestoegang en schrijftoegang afzonderlijk worden toegestaan of geweigerd.

HP Device Access Manager wordt automatisch ingesteld met de volgende instellingen tijdens het afronden van de HP Client Security Setup Wizard:

- Just In Time Authentication (JITA) Removable Media is ingeschakeld voor beheerders en gebruikers.
- Het apparaatbeleid staat volledige toegang tot andere apparaten toe.

Device Access Manager openen

1. Klik of tik op het startscherm op de app **HP Client Security** (Windows 8).

   – of –

   Dubbelklik of dubbeltik op het bureaublad van Windows op het pictogram **HP Client Security** in het systeemvak, rechts op de taakbalk.

2. Klik of tik onder **Device** (Apparaat) op **Device Permissions** (Apparaatmachtigingen).

   - Standaardgebruikers kunnen hun actuele apparaattoegang bekijken (zie Gebruikersweergave op pagina 45).
   - Beheerders kunnen de apparaattoegang bekijken en wijzigen die op dat moment is ingesteld voor de computer door op **Change** (Wijzigen) te tikken of klikken en vervolgens het beheerderswachtwoord in te voeren (zie Systeemweergave op pagina 45).

Gebruikersweergave

Als **Device Permission** (Apparaatmachtiging) is geselecteerd, wordt de Gebruikersweergave getoond. Afhankelijk van het beleid kunnen standaardgebruikers en beheerders hun eigen toegang bekijken voor apparaatklassen of individuele apparaten van deze computer.

- **Current user** (Huidige gebruiker): de naam van de aangemelde gebruiker wordt weergegeven.
- **Device Class** (apparaatklasse): de soorten apparaten worden weergegeven.
- **Access IToegang)**: uw actueel ingestelde toegang tot soorten apparaten of specifieke apparaten wordt weergegeven.
- **Duration** (Duur): de tijdslimiet voor uw toegang tot cd/dvd-rom stations of verwisselbare schijven wordt weergegeven.
- **Settings** (Instellingen): beheerders kunnen veranderen voor welke schijfeenheden de toegang beheerd wordt door Device Access Manager.

Systeemweergave

In de systeemweergave kunnen beheerders toegang toekennen of weigeren voor apparaten op deze computer voor de groep Gebruikers of de groep Beheerders.

▲ Beheerders kunnen de systeemweergave openen door op **Change** (Wijzigen) te klikken of tikken, een beheerderswachtwoord in te voeren, en een keuze te maken uit de volgende opties:

- **Device Access Manager**: om HP Device Access Manager met Just In Time Authentication in of uit te schakelen, klik of tik op **On** (Aan) of **Off** (Uit).
- **Users and groups on this PC** (Gebruikers en groepen op deze pc): geeft de groep Gebruikers of de groep Beheerders weer die wel of geen toegang hebben tot de geselecteerde apparaatklassen.
- **Device Class** (apparaatklasse): geeft de apparaatklassen en apparaten weer die in het systeem zijn geïnstalleerd of die mogelijk eerder op het systeem waren geïnstalleerd. Klik op het pictogram **+** om de lijst uit te vouwen. Alle met de computer verbonden apparaten worden weergegeven en de groepen Beheerders en Gebruikers zijn uitgevouwen zodat de leden

zichtbaar zijn. Klik op het pictogram met de ronde pijl (vernieuwen) om de lijst met apparaten bij te werken.

- Voor een apparaatklasse is meestal beveiliging toegepast. Als toegang is ingesteld op **Allow** (Toestaan), kan de geselecteerde gebruiker of groep elk apparaat in de apparaatklasse benaderen.
- Beveiliging kan ook worden toegepast voor specifieke apparaten.
- Stel Just In Time authentication (JITA) in waardoor geselecteerde gebruikers toegang krijgen tot cd/dvd-rom stations of verwisselbare schijven door zichzelf te verifiëren. Zie JITA-configuratie op pagina 46 voor meer informatie.
- Gun of weiger toegang tot andere apparaatklassen zoals verwisselbare media (zoals USB-sticks) seriële en parallelle poorten, Bluetooth®-apparaten, modems, PCMCIA/ExpressCard-apparaten, 1394-apparaten, vingerafdruklezer en smartcardlezer. Als toegang tot de vingerafdruklezer en de smartcardlezer geweigerd worden, kunnen ze worden toegepast als verificatiereferentie maar zijn ze niet bruikbaar op sessie beleidsniveau.

OPMERKING: Als Bluetooth-apparaten gebruikt worden als verificatiereferentie, mag de toegang tot Bluetooth-apparaten niet worden beperkt in het beleid van Device Access Manager.

- Als u een instelling selecteert op het niveau van groep of apparaatklasse, en u wordt gevraagd of u de instelling wilt toepassen op de onderliggende objecten:

  Ja: de instelling wordt gepropageerd.

  Nee: de instelling wordt niet gepropageerd.

- Sommige apparaatklassen, zoals dvd en cd-rom, kunnen verder beheerd worden door toegang afzonderlijk toe te staan of te weigeren voor lees- en schrijfhandelingen.

OPMERKING: De groep Beheerders kan niet worden toegevoegd aan de lijst Gebruikers.

- **Access** (Toegang): klik of tik op het pijltje omlaag en selecteer een van de volgende toegangssoorten om toegang toe te staan of te weigeren:
  - **Allow – Full Access** (Toestaan - Volledige toegang)
  - **Allow – Read Only** (Toestaan - Alleen schrijven)
  - **Allow – JITA Required** (Toestaan - JITA vereist): zie JITA-configuratie op pagina 46 voor meer informatie.

    Als dit type toegang is geselecteerd, klikt of tikt u onder **Duration** (Duur) op het pijltjeomlaag om een tijdslimiet te selecteren.
  - **Deny** (Weigeren)
- **Duration** (Duur): klik of tik op het pijltje omlaag om een tijdslimiet in te stellen voor toegang tot cd/dvd-rom stations of verwisselbare schijven (zie JITA-configuratie op pagina 46).

JITA-configuratie

JITA-configuratie stelt de beheerder in staat om lijsten met gebruikers en groepen te bekijken en bewerken die toestemming hebben om apparaten te benaderen met Just In Time Authentication (JITA).

Gebruikers kunnen met JITA toegang krijgen tot een aantal apparaten waarvoor beperking is ingesteld in beleiden gemaakt in de weergave **Device Class Configuration** (Configuratie apparaatklasse).

De JITA-periode kan worden geautoriseerd voor een bepaald aantal minuten of onbeperkt. Onbeperkte gebruikers hebben toegang tot het apparaat vanaf het moment dat zij zich verifiëren tot het moment dat ze zich bij het systeem afmelden.

Als de gebruiker een beperkte JITA-periode heeft gekregen, wordt de gebruiker een minuut voor het verstrijken van de JITA-periode gevraagd of de toegang verlengd moet worden. Zodra de gebruiker zich afmeldt bij het systeem of een andere gebruiker meldt zich aan, verloopt de JITA-periode. De volgende keer dat de gebruiker zich aanmeldt en probeert om een apparaat onder JITA te bereiken, verschijnt een vraag voor het invoeren van de referenties.

JITA is beschikbaar voor de volgende apparaatklassen:

- Dvd/cd-rom stations
- Verwisselbare schijfstations

Een JITA-beleid maken voor een gebruiker of groep

Beheerders kunnen gebruikers of groepen toegang geven of weigeren tot apparaten met Just In Time Authentication (JITA).

1. Start **Device Access Manager** en klik of tik op **Change** (Wijzigen).
2. Selecteer de gebruiker of groep en klik of tik op het pijltje omlaag onder **Access** (Toegang) voor **Removable Disk drives** (Verwisselbare schijfstations) of **DVD/CD-ROM drives** (Dvd/cd-rom stations) en selecteer **Allow – JITA Required** (Toestaan - JITA verplicht).
3. Klik of tik onder **Duration** (Duur) op het pijltje omlaag om een periode voor JITA-toegang te selecteren.

De gebruiker moet zich af- en weer aanmelden om de nieuwe JITA-instelling toe te passen.

Een JITA-beleid voor een gebruiker of groep uitschakelen

Beheerders kunnen toegang door gebruikers of groepen tot apparaten met Just In Time Authentication (JITA) uitschakelen.

1. Start **Device Access Manager** en klik of tik op **Change** (Wijzigen).
2. Selecteer de gebruiker of groep en klik of tik op het pijltje omlaag onder **Access** (Toegang) voor **Removable Disk drives** (Verwisselbare schijfstations) of **DVD/CD-ROM drives** (Dvd/cd-rom stations) en selecteer **Deny** (Weigeren).

Als de gebruiker zich aanmeldt en probeert om het apparaat te gebruiken, wordt de toegang geweigerd.

Instellingen

De weeergave **Instellingen** stelt beheerders in staat om de stations te bekijken en te wijzigen waarvoor de toegang beheerd wordt door Device Access Manager.

OPMERKING: Device Access Manager moet actief zijn als de lijst met stationsletters wordt geconfigureerd (zie Systeemweergave op pagina 45).

Onbeheerde apparaatklassen

HP Device Access Manager beheert de volgende apparaatklassen niet:

- In- en uitvoerapparaten
  - CD-ROM
  - Schijfstation
  - Floppy disk controller (FDC)
  - Hard disk controller (HDC)
  - Human interface device (HID) klasse
  - Infrarode human interface apparaten
  - Muis
  - Multi-poort serieel
  - toetsenbord
  - Plug and play (PnP) printers
  - Printer
  - Printer upgrade
- Aan/uit
  - Ondersteuning voor geavanceerd energiebeheer (APM)
  - Accu
- Varia
  - Computer
  - Decoder
  - Beeldscherm
  - Intel® unified display driver
  - Legacard
  - Media-stuurprogramma
  - Mediawisselaar
  - Geheugentechnologie
  - Monitor
  - Multifunctie
  - Net client
  - Net service
  - Net trans
  - Processor
  - SCSI-adapter

- Beveiligings-accelerator
- Beveiligingsapparaten
- Systeem
- Onbekend
- Volume
- Volume snapshot

8 HP Trust Circles

HP Trust Circles is een applicatie voor het beveiligen van bestanden en documenten waarin coderen van mappen en bestanden gecombineerd is met een handige mogelijkheid om documenten te delen met een "vertrouwde kring". De applicatie codeert bestanden die geplaatst zijn in door de gebruiker opgegeven mappen en beschermt ze binnen een vertrouwde kring. Eenmaal beschermd kunnen de bestanden uitsluitend worden gebruikt en gedeeld door leden in de vertrouwenskring. Als een beschermd bestand ontvangen wordt door iemand die geen lid is, blijft het bestand gecodeerd en kan het niet-lid de inhoud niet openen.

Trust Circles openen

1. Klik of tik op het startscherm op de app **HP Client Security**.

   – of –

   Dubbelklik of dubbeltik op het bureaublad van Windows op het pictogram **HP Client Security** in het systeemvak, rechts op de taakbalk.

2. Klik of tik onder **Data** op **Trust Circles**.

Aan de slag

Er zijn twee manieren om uitnodigingen per e-mail te verzenden en beantwoorden:

- **Met Microsoft® Outlook**: door Trust Circles te gebruiken met Microsoft Outlook automatiseert u het verwerken van alle Trust Circle-uitnodigingen en -antwoorden van andere Trust Circle-gebruikers.
- **Met Gmail, Yahoo, Outlook.com of andere e-maildiensten (SMTP)**: als u uw naam, e-mailadres en wachtwoord invoert, gebruikt Trust Circles uw e-maildienst om e-mailuitnodigingen te sturen naar geselecteerde leden om zich bij uw trust circle te voegen.

Uw basisprofiel instellen

1. Voer uw naam en e-mailadres in en klik of tik op **Volgende**.

   De naam is zichtbaar voor alle leden die uitgenodigd zijn om zich bij uw trust circle te voegen. Het e-mailadres wordt gebruikt om uitnodigingen te verzenden, ontvangen of beantwoorden.

2. Typ het wachtwoord voor de e-mailaccount en klik of tik op **Volgende**.

   Een test e-mail wordt verzonden om er voor te zorgen dat de e-mailinstellingen nauwkeurig zijn.

   OPMERKING: De computer moet verbonden zijn met een netwerk.

3. Voer in het veld **Trust Circle Name** (Trust Circle naam) een naam in voor de trust circle en klik of tik op **Volgende**.

4. Voeg leden en mappen toe en klik of tik op **Volgende**. De trust circle wordt opgezet met alle geselecteerde mappen en stuurt e-mailuitnodigingen naar alle geselecteerde leden. Als een uitnodiging om enige reden niet kan worden verzonden, wordt een melding weergegeven. Leden kunnen op elk moment opnieuw worden uitgenodigd vanuit de weergave Trust Circle door te

klikken op **Your Trust Circles** (Uw Trust Circles) en vervolgens op de trust circle te dubbelklikken of dubbeltikken. Zie Trust Circles op pagina 51 voor meer informatie.

Trust Circles

U kunt een trust circle maken tijdens de eerste installatie nadat u uw e-mailadres hebt opgegeven, of in de weergave Trust Circle:

▲ Klik of tik in de weergave Trust Circle op **Create Trust Circle** (Trust Circle maken) en typ een naam voor de trust circle.

- Om leden toe te voegen aan de trust circle klikt of tikt u op het pictogram **M+** naast **Members** (Leden) waarna u de aanwijzingen op het scherm volgt.
- Om mappen toe te voegen aan de trust circle klikt of tikt u op het pictogram **+** naast **Folders** (Mappen) en de instructies op het scherm te volgen.

Mappen toevoegen aan een trust circle

Mappen toevoegen aan een nieuwe trust circle

- Tijdens het maken van een trust circle kunt u mappen toevoegen door te klikken of tikken op het pictogram **+** naast **Folders** (Mappen) en de instructies op het scherm te volgen.

  – of –

- rechtsklik of tik in Windows Verkenner op een map die nog geen deel uitmaakt van een trust circle, selecteer **Trust Circle** en selecteer vervolgens **Create Trust Circle from Folder** (Trust Circle van map maken).

TIP: U kunt een of meer mappen selecteren.

Mappen toevoegen aan een bestaande trust circle

- Klik of tik in de weergave Trust Circle op **Your Trust Circles** (Uw Trust Circles), dubbelklik of dubbeltik op de bestaande trust circle om de actuele mappen weer te geven, klik of tik op het pictogram **+** naast **Folders** (Mappen) en de instructies op het scherm te volgen.

  – of –

- rechtsklik of tik in Windows Verkenner op een map die nog geen deel uitmaakt van een trust circle, selecteer **Trust Circle** en selecteer vervolgens **Add to existing Trust Circle from Folder** (Aan bestaande Trust Circle toevoegen vanuit map).

TIP: U kunt een of meer mappen selecteren.

Nadat een map is toegevoegd aan een trust circle, codeert Trust Circles automatisch de map en de inhoud. Nadat alle bestanden gecodeerd zijn, wordt een melding weergegeven. Verder verschijnt een groen symbool van een slot op alle pictogrammen van gecodeerde mappen en bestanden binnen de mappen om aan te geven dat ze volledig gecodeerd zijn.

Leden toevoegen aan een trust circle

In drie stappen voegt u leden toe aan een trust circle:

1. **Uitnodigen**: eerst nodigt de eigenaar van de trust circle de leden uit. De uitnodigings e-mail kan verzonden worden naar meerdere gebruikers of distributielijsten/groepen.
2. **Accepteren**: de genodigde ontvangt de uitnodiging en bepaalt of deze wel of niet wordt geaccepteerd. Als de genodigde de uitnodiging accepteert, ontvangt de uitnodiger een e-mail met het antwoord. Als de uitnodiging naar een groep is gezonden, ontvangt elk lid een uitnodiginig en kiest of deze wel of niet geaccepteerd wordt.
3. **Inschrijven**: de uitnodiger heeft een laatste kans om te bepalen of het lid aan de trust circle moet worden toegevoegd. Als de uitnodiger besluit om het lid in te schrijven, ontvangt de genodigde een e-mail met een bevestiging van het antwoord. De uitnodiger en genodigde kunnen optioneel de beveiliging van het uitnodigingsproces verifiëren. Voor de genodigde wordt een verificatiecode weergegen, die telefonisch aan de uitnodiger moet worden voorgelezen. Nadat de code is geverifieerd, kan de uitnodiger de laatste inschrijvings e-mail sturen.

Leden toevoegen aan een nieuwe trust circle

▲ Tijdens het maken van een trust circle kunt u leden toevoegen door te klikken of tikken op het pictogram **M+** naast **Members** (Leden) en de instructies op het scherm te volgen.

- Als u Outlook gebruikt: selecteer contactpersonen in het adressenboek van Outlook en klik op **OK**
- Als u een andere e-maildienst gebruikt, kunt u handmatig nieuwe e-mailadressen toevoegen aan Trust Circle of u kunt ze laten ophalen uit de e-mailadressen die op Trust Circle zijn geregistreerd.

Leden toevoegen aan een bestaande trust circle

▲ Klik of tik in de weergave Trust Circle op **Your Trust Circles** (Uw Trust Circles), dubbelklik of dubbeltik op de bestaande trust circle om de actuele mappen weer te geven, klik of tik op het pictogram **M+** naast **Members** (Leden) en de instructies op het scherm te volgen.

- Als u Outlook gebruikt: selecteer contactpersonen in het adressenboek van Outlook en klik op **OK**.
- Als u een andere e-maildienst gebruikt, kunt u handmatig nieuwe e-mailadressen toevoegen aan Trust Circle of u kunt ze laten ophalen uit de e-mailadressen die op Trust Circle zijn geregistreerd.

Bestanden toevoegen aan een trust circle

U kunt op de volgende manieren bestanden toevoegen aan een trust circle:

- Kopieer of verplaats het bestand naar een bestaande trust circle-map.

  – of –

- Rechtsklik of -tik In Windows Verkenner op een bestand dat is momenteel niet gecodeerd en houd dit vast, selecteer **Trust Circle** (Vertrouwenscirkel) en selecteer **Encrypt** (Coderen). U wordt gevraagd om de trust circle te selecteren waaraan het bestand moet worden toegevoegd.

TIP: U kunt een of meer bestanden selecteren.

Gecodeerde mappen

Ieder lid van een trust circle kan bestanden bekijken en bewerken die tot die trust circle behoren.

OPMERKING: Trust Circle Manager/Reader synchroniseert geen bestanden tussen leden.

Bestanden moeten via bestaande methoden worden gedeeld, zoals e-mail, ftp of opslag in de cloud. Bestanden die gekopieerd worden naar, verplaatst naar of gemaakt in een trust circle-map worden direct beveiligd.

Mappen verwijderen uit een trust circle

Door een map te verwijderen uit een trust circle, wordt de map met de gehele inhoud gedecodeerd en de beveiliging verwijderd.

- Klik of tik in de weergave Trust Circle op **Your Trust Circles** (Uw Trust Circles), dubbelklik of dubbeltik op de bestaande trust circle om de actuele mappen weer te geven, klik of tik op het pictogram **prullenbak** naast die map.

  – of –

- rechtsklik of tik in Windows Verkenner op een map die deel uitmaakt van een trust circle, selecteer **Trust Circle** en selecteer vervolgens **Remove from trust circle** (Uit Trust Circle verwijderen).

TIP: U kunt een of meer mappen selecteren.

Een bestand verwijderen uit een trust circle

Om een bestand te verwijderen uit een trust circle, rechtsklikt of tikt u in Windows Verkenner op een bestand dat is gecodeerd; selecteer **Trust Circle**, selecteer **Decrypt File** (Bestand decoderen).

Leden verwijderen uit een trust circle

Een volledig ingeschreven lid kan niet worden verwijderd uit een trust circle. Een alternatief is het maken van een nieuwe trust circle met alle andere leden, alle bestanden en mappen naar de nieuwe trust circle verplaaten en de oude trust circle verwijderen. Dit zorgt er voor dat alle nieuwe bestanden die het lid ontvangt, niet toegankelijk is, maar dat alles dat eerder was gedeeld, toegankelijk blijft voor het lid van de oude trust circle.

Als een lid niet volledig is ingeschreven (het lid is uitgenodigd om zich bij de trust circle te voegen of heeft de uitnodiging voor de trust circle niet geaccepteerd) kunt u het lid op een van de volgende manieren verwijderen uit de trust circle:

- Klik of tik in de weergave Trust Circle op **Your Trust Circles** (Uw Trust Circles), en dubbelklik of dubbeltik op de trust circle om de actuele ledenlijst weer te geven. Klik of tik op het pictogram **prullenbak** naast de naam van het lid dat u wilt verwijderen.
- Klik of tik in de weergave Trust Circle op **Members** (Leden) en dubbelklik of dubbeltik op het lid om de trust circles weer te geven waar hij of zij lid van is. Klik of tik op het pictogram **prullenbak** naast een trust om het lid uit die trust circle te verwijderen.

Een trust circle verwijderen

Om een trust circle te kunnen verwijderen, moet u daar de eigenaar van zijn.

▲ Klik of tik in de weergave Trust Circle op **Your Trust Circles** (Uw Trust Circles), klik of tik op het pictogram **prullenbak** naast de te verwijderen trust circle.

Dit verwijdert de trust circle van de pagina en stuurt e-mails naar alle leden van de trust circle om ze op de hoogte te brengen dat de trust circle verwijderd is. Alle bestanden of mappen in die trust circle worden gedecodeerd.

Voorkeuren instellen

Klik of tik in de weergave Trust Circle op **Preferences** (Voorkeuren). Drie tabs verschijnen

- **E-mail instellingen**

Optie	Beschrijving
Username (Gebruikersnaam)	De gebruikte gebruikersnaam wordt weergegeven. Om deze te wijzigen, typt u een nieuwe gebruikersnaam in het tekstvak. Wijzigingen worden automatisch opgeslagen.
Email Address (E-mailadres)	Het actueel gebruikte e-mailadres wordt weergegeven. Klik of tik op **Change Email Settings** (E-mailinstellingen wijzigen) om het te veranderen en volg de instructies op het scherm.
New Member Confirmation (Bevestiging nieuw lid)	Kies uit de volgende opties: ◦ **Confirm Automatically** (Automatisch bevestigen): na ontvangst van een acceptatie door (een) genodigde(n) vindt bevestiging plaats in de trust circle zonder handmatige invoer en wordt een bevestigings e-mail naar de genodigde(n) gezonden. ◦ **Confirm Manually** (Handmatig bevestigen): na ontvangst van een acceptatie door (een) genodigde(n) is handmatige invoer vereist om de nieuwe leden toe te voegen aan de trust circle, waarna een bevestigings e-mail wordt verzonden. ◦ **Require Verification** (Verificatie verplicht): na ontvangst van een acceptatie door (een) genodigde(n) is een verificatiecode nodig om de genodigde(n) volledig in te schrijven. De eigenaar van de trust circle moet contact opnemen met de genodigde(n) en de verificatiecode ontvangen. Na invoer van de verificatiecode worden de bevestigingen verzonden.
Periodic Authentication (Periodieke verificatie)	Bij periodieke verificatie moet de gebruiker na een ingestelde time-out (vastgelegd in minuten) om het wachtwoord voor Windows in te voeren, en eveneens bij het uitvoeren van gevoelige handelingen. Gebruikers kunnen deze verificatie in- of uitschakelen.
Authentication Timeout (Time-out voor verificatie)	Selecteer de opgegeven time-out periode (vastgelegd in minuten) voordat verificatie verplicht is.
Don't show confirmation message (Bevestigingsbericht niet weergeven)	Selecteer het selectievakje om de weergave van bevestigingen uit te schakelen of wis het selectievakje om weergave in te schakelen.
I'd like to help improve the HP Trust Circle through anonymous usage tracking (Ik wil de HP Trust Circle helpen verbeteren via het anoniem volgen van het gebruik)	Selecteer het selectievakje om deel te nemen aan het programma of wis het selectievakje als u niet wilt deelnemen.

- **Back-up/herstellen**

Optie	Beschrijving
Back-up	Kopieert uw applicatiegegevens van Trust Circle Manager/Reader (instellingen en trust circles) naar een back-upbestand. In het geval van een crash of systeemfout kunt u dit bestand gebruiken om de nieuwe installatie van Trust Circles te herstellen tot de staat die in het bestand is opgeslagen. **OPMERKING:** Alleen de Trust Circle-applicatiegegevens worden opgeslagen (trust circles, instellingen en leden). Van de eigenlijke bestanden in de trust circle-mappen wordt geen back-up gemaakt. Van die bestanden moet u een aparte back-up maken. Back-up maken van Trust Circle-instellingen en gebruikersgegevens: **1.** Klik of tik op **Backup** (Back-up). **2.** Kies een bestandsnaam en map voor het back-upbestand en klik of tik op **Save** (Opslaan). **3.** Typ een wachtwoord, bevestig dit en klik of tik op **OK**. Dit wachtwoord is nodig om het bestand te herstellen.
Herstellen	Herstelt instellingen en trust circles uit een back-upbestand, gewoonlijk na een systeemcrash of migratie naar een andere computer. De instellingen en gebruikersgegevens van Trust Circle herstellen: **1.** Klik of tik op **Restore** (Herstellen). **2.** Ga naar de map en de bestandsnaam van het back-upbestand en klik of tik op **Open** (Openen). **3.** Typ het wachtwoord dat bij het maken van de back-up was ingesteld.

- **About** (Over): de versie van de Trust Circle Manager/Reader software wordt weergegeven. Koppelingen worden weergegeven waarmee u Trust Circle Manager kunt opwaarderen naar de Pro-versie of om het privacybeleid van HP weer te geven.

9 Theft recovery (alleen bepaalde modellen)

Met Computrace (afzonderlijk aan te schaffen) kunt u op afstand uw computer bewaken, beheren en traceren.

Eenmaal geactiveerd wordt Computrace ingesteld vanuit het Absolute Software Customer Center. In het Customer Center kan de beheerder Computrace instellen om de computer te bewaken of beheren. Als het systeem kwijtgeraakt is of wordt gestolen, kan het Customer Center de lokale overheid helpen bij het localiseren en terughalen van de computer. Indien geconfigureerd, kan Computrace blijven functioneren zelfs als de harde schijf is gewist of vervangen.

Zo activeert u Computrace:

1. Maak verbinding met internet.
2. Open HP Client Security. Zie HP Client Security openen op pagina 10 voor meer informatie.
3. Klik op **Theft Recovery** (Terughalen na diefstal).
4. Om de activeringswizard voor Computrace te starten, klikt u op **Get Started** (Aan de slag).
5. Voer uw contactinformatie en uw credit card-gegevens in of voer een vooraf aangeschaft productidentificatienummer in.

De activeringswizard zorgt voor een beveiligde verwerking van de transactie en stelt uw gebruikersaccount in op de Absolute Software Customer Center-website. Na voltooiing ontvangt u een bevestigings e-mail met uw Customer Center-accountgegevens.

Als u al eerder de activeringswizard voor Computrace hebt uitgevoerd en uw Customer Center-gebruikersaccount bestaat al, kunt u extra licenties aanschaffen door contact op te nemen met uw HP accountvertegenwoordiger.

Zo meld u zich aan bij het Customer Center:

1. Ga naar https://cc.absolute.com/.
2. Typ in de velden **Login ID** (aanmeld-ID) en **Password** (Wachtwoord) de aanmeldgegevens die u hebt ontvangen in de bevestigings e-mail en klik op **Log in** (Aanmelden).

Met behulp van het Customer Center kunt u:

- Uw computers bewaken.
- Uw externe gegevens beschermen.
- De diefstal melden van elke computer die beveiligd wordt door Computrace.

▲ Klik op **Learn More** (Meer informatie) voor meer informatie over Computrace.

10 Gelokaliseerde uitzonderingen voor wachtwoorden

Op het niveau van Opstartverificatie en HP Drive Encryption is ondersteuning voor wachtwoordlocalisatie beperkt. Zie Windows IME's niet ondersteund op het verificatieniveau Opstartverificatie of het niveau van Drive Encryption op pagina 57 voor meer informatie.

Wat te doen als een wachtwoord wordt verworpen

Wachtwoorden kunnen om de volgende redenen verworpen worden:

- Een gebruiker werkt met een IME die niet wordt ondersteund. Dit komt veel voor bij dubbel-byte talen (Koreaans, Japans, Chinees). Om dit probleem op te lossen:

  1. Voeg met het **Configuratiescherm** een ondersteunde toetsenbordindeling toe (voeg US/ Engelse toetsenborden toe onder Chinese invoer taal).
  2. Stel het ondersteunde toetsenbord in voor standaard invoer.
  3. Start HP Client Security en voer het Windows-wachtwoord in.

- Een gebruiker gebruikt een teken dat niet wordt ondersteund. Om dit probleem op te lossen:

  1. Verander het Windows-wachtwoord zodat dit alleen ondersteunde tekens bevat. Zie voor meer informatie over niet-ondersteunde tekens Verwerking bijzondere toetsen op pagina 58.
  2. Start HP Client Security en voer het Windows-wachtwoord in.

Windows IME's niet ondersteund op het verificatieniveau Opstartverificatie of het niveau van Drive Encryption

Onder Windows kan een gebruiker een IME (invoer methode editor) kiezen om complexe tekens en symbolen in te voeren, zoals Japanse of Chinese tekens, met behulp van een standaard westers toetsenbord.

IME's worden niet ondersteund op het niveau van Opstartverificatie of Drive Encryption. Een Windows-wachtwoord kan niet worden ingevoerd met een IME in het aanmeldvenster voor Opstartverificatie of HP Drive Encryption; als dit toch gebeurt, kan de gebruiker worden uitgesloten. In sommige gevallen toont Microsoft® Windows niet het scherm IME wanneer de gebruiker het wachtwoord typt.

De oplossing is om naar een van de volgende ondersteunde toetsenbordindelingen te wisselen die toetsenbordindeling 00000411 ondersteunt.

- Microsoft IME voor Japans
- De Japanse toetsenbordindeling
- Office 2007 IME vor Japans: als Microsoft of een derde partij de term IME of input method editor gebruikt, is de invoermethode mogelijk niet echt een IME. Dat kan verwarring wekken maar de

software leest de weergave van de hexadecimale code. Als een IME daarom verwijst naar een ondersteunde toetsenbordindeling, kan HP Client Security de configuratie ondersteunen.

⚠ **WAARSCHUWING!** Als HP Client Security gebruikt wordt, worden wachtwoorden verworpen die met een Windows IME worden ingevoerd.

Wachtwoordwijzigingen met een toetsenbordindeling die eveneens wordt ondersteund

Als het wachtwoord aanvankelijk is ingesteld met een toetsenbordindeling zoals U.S. English (409), waarna de gebruiker het wachtwoord verandert met een andere toetsenbordindeling die eveneens wordt ondersteund, zoals Latin American (080A) werkt de wachtwoordwijziging in HP Drive Encryption maar niet in het BIOS als de gebruiker tekens toepast die wel in de laatste maar niet in de eerste voorkomen (bijvoorbeeld ē).

OPMERKING: Beheerders kunnen dit probleem oplossen met de pagina Users (Gebruikers) van HP Client Security (bereikbaar vanaf het **tandwiel** pictogram op de startpagina) om de gebruiker te verwijderen uit HP Client Security, de gewenste toetsenbordindeling te kiezen in het besturingssysteem, en daarna de HP Client Security Setup Wizard nogmaals uit te voeren voor dezelfde gebruiker. Het BIOS slaat de gewenste toetsenbordindeling op en wachtwoorden die getypt kunnen worden met deze toetsenbordindeling worden correct ingesteld in het BIOS.

Een ander mogelijk probleem is het gebruik van verschillende toetsenbordindelingen die alle dezelfde tekens kunnen produceren. Zo kunnen bijvoorbeeld zowel de toetsenbordindeling U.S. International (20409) als de toetsenbordindeling Latin American (080A) het teken é produceren, al kunnen daar verschillende toetsencombinaties voor nodig zijn. Als een wachtwoord oorspronkelijk is ingesteld met de toetsenbordindeling Latin American, dan is de toetsenbordindeling Latin American ingesteld in het BIOS, ook al wordt het wachtwoord later gewijzigd met de toetsenbordindeling U.S. International.

Verwerking bijzondere toetsen

- Chinees, Slowaaks, Canadees-Frans en Tsjechisch

  Wanneer een gebruiker een van de voorgaande toetsenbordindelingen selecteert en een wachtwoord typt (bijvoorbeeld abcdef), moet hetzelfde wachtwoord worden ingevoerd terwijl u de shift-toets indrukt voor kleine letters en de toetsen shift en caps lock voor hoofdletters in de opstartverificatie en HP Drive Encryption. Numerieke wachtwoorden moeten met het numerieke toetsenblok worden ingevoerd.

- Koreaans

  Als een gebruiker een ondersteunde Koreaanse toetsenbordindeling selecteert en een wachtwoord typt (bijvoorbeeld abcdef), moet hetzelfde wachtwoord worden ingevoerd terwijl u de alt-toets indrukt voor kleine letters en de toetsen alt en caps lock voor hoofdletters in de opstartverificatie en HP Drive Encryption.

- De volgende tabel geeft een overzicht van niet-ondersteunde tekens:

Language (Taal)	Windows	BIOS	Drive Encryption
Arabisch	De toetsen ﻻ ,ﻷ, en ﻹ genereren twee tekens.	De toetsen ﻻ ,ﻷ, en ﻹ genereren een teken.	De toetsen ﻻ ,ﻷ, en ﻹ genereren een teken.
Canadees-Frans	ç, è, à en é met caps lock zijn Ç, È, À en É in Windows.	ç, è, à, en é met caps lock zijn ç, è, à en é in de opstartverificatie.	ç, è, à, en é met caps lock zijn ç, è, à é in HP Drive Encryption.

Language (Taal)	Windows	BIOS	Drive Encryption
Spaans	40a wordt niet ondersteund. Toch werkt dit, omdat de software dit converteert naar c0a. Als gevolg van subtiele verschillen in de toetsenbordindelingen wordt echter aanbevolen dat Spaans sprekende gebruikers hun Windows toetsenbordindeling veranderen naar 1040a (Spanish Variation) of 080a (Latin American).	n.v.t.	n.v.t.
US international	◦ De toetsen ¡, ¤, ‘, ’, ¥ en × op de bovenste rij worden verworpen. ◦ De toetsen å, ® en Þ op de tweede rij worden verworpen. ◦ De toetsen á, ð en ø op de derde rij worden verworpen. ◦ De toets æ op de onderste rij wordt verworpen.	n.v.t.	n.v.t.
Tsjechisch	◦ De toets ğ wordt verworpen. ◦ De toets į wordt verworpen. ◦ De toets ų wordt verworpen. ◦ De toetsen ė, ı en ż worden verworpen. ◦ De toetsen ģ, ķ, ļ, ņ en ţ worden verworpen.	n.v.t.	n.v.t.
Slowaaks	De toets ż wordt verworpen.	◦ De toetsen š, ś en ş worden verworpen als ze worden getypt, maar ze worden wel geaccepteerd als ze worden ingevoerd met het schermtoetsenbord. ◦ De dode toets ţ genereert twee tekens.	n.v.t.
Hongaars	De toets ż wordt verworpen.	De toets ţ genereert twee tekens.	n.v.t.

Language (Taal)	Windows	BIOS	Drive Encryption
Sloveens	De toets żŻ wordt verworpen in Windows en de alt-toets genereert een dode toets in het BIOS.	De toetsen ú, Ú, ů, Ů, ş, Ş, ś, Ś, š en Š worden verworpen in het BIOS.	n.v.t.
Japans	Indien beschikbaar is Microsoft Office 2007 IME een betere keuze. Ondanks de naam IME is het in feite toetsenbordindeling 411, die ondersteund wordt.	n.v.t.	n.v.t.

Woordenlijst

aangesloten apparaat
Een hardwareapparaat dat is aangesloten op een poort van de computer.

aanmelden
Een object binnen HP Client Security dat bestaat uit een gebruikersnaam en wachtwoord (en eventueel andere geselecteerde informatie) die gebruikt kan worden om u aan te melden op websites of bij andere programma's.

activering
De taak die moet worden uitgevoerd voordat de functies van Drive Encryption beschikbaar zijn. Beheerders kunnen Drive Encryption activeren met de HP Client Security Setup Wizard of met HP Client Security. Het activeringsproces bestaat uit het activeren van de software, het coderen van de schijfeenheid, en het maken van de eerste back-up van de coderingssleutel op een verwisselbaar opslagapparaat.

apparaatklasse
Alle apparaten van een bepaald type, zoals schijfeenheden.

automatische versnippering
vernietigen dat u automatiseert in File Sanitizer.

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

beheerder
Zie *Windows beheerder*.

beveiligde aanmeldingsmethode
De methode die wordt gebruikt voor het aanmelden op de computer.

Bluetooth
Technologie die radiotransmissies gebruikt om computers, printers, muizen, mobiele telefoons en andere apparaten met Bluetooth-ondersteuning radiocommunicatie te bieden over een korte afstand.

contactloze kaart
Een plastic kaart met een computerchip die voor verificatie bruikbaar is.

decodering
Een procedure gebruikt in cryptografie gecodeerde gegevens om te zetten naar platte tekst.

domein
Een groep computers die deel uitmaken van een netwerk en die een gemeenschappelijke directory database delen. Domeinen hebben een unieke naam en elk heeft een reeks gemeenschappelijke regels en procedures.

Drive Encryption
Beschermt uw gegevens door uw vaste schijf of schijven te coderen, waardoor de informatie onleesbaar wordt voor mensen die niet over de benodigde toestemming beschikken.

Drive Encryption aanmeldingsscherm
Zie verificatie voorafgaand aan opstarten voor Drive Encryption

Drive Encryption verificatie voorafgaand aan opstarten
Een aanmeldvenster dat verschijnt voordat Windows start. Gebruikers moeten hun gebruikersnaam en wachtwoord voor Windows invullen of hun pincode van een smartcard, of met een vastgelegde vinger vegen.

Als aanmelden in één stap is geselecteerd, is na invoeren van de juiste informatie in het aanmeldvenster van Drive Encryption rechtstreeks toegang mogelijk tot Windows zonder dat opnieuw moet worden ingelogd in het aanmeldvenster van Windows.

DriveLock
Een beveiligingsfunctie die de harde schijf koppelt aan een gebruiker en die vereist dat de gebruiker het DriveLock-wachtwoord typt als de computer opstart.

Encryption File System (EFS)
Een systeem dat alle bestanden en submappen binnen de geselecteerde map codeert.

gebruiker
Iedereen die geregistreerd is in Drive Encryption. Andere gebruikers dan beheerders hebben beperkte rechten in Drive Encryption. Zij kunnen zich alleen registreren (met goedkeuring van de beheerder) en aanmelden.

gegevensbestanddeel
Een gegevenscomponent bestaande uit persoonlijke gegevens of bestanden, historische en webgerelateerde gegevens, enzovoort die zich op de harde schijf bevinden.

groep
Een groep gebruikers met hetzelfde niveau van toegang of weigering voor een apparaatklasse of een specifiek apparaat.

handmatige versnippering
Direct vernietigen van een gegevenselement of geselecteerde gegevenselementen, waarbij een geplande actie genegeerd wordt.

hardwarecodering
Het gebruik van zelfcoderende schijfeenheden die voldoen aan de OPAL-specificatie van de Trusted Computing Group voor het beheren van zelfcoderende schijven voor een volledige directe codering. Hardwarecodering werkt direct en duurt hoogstens een paar minuten, maar softwarecodering kan meerdere uren duren.

herstart
Het proces van het herstarten van de computer.

herstellen
Een proces dat programmainformatie kopieert van een eerder opgeslagen back-up naar dit programma.

HP SpareKey terugzetten
Toegang krijgen tot uw computer door beveiligingsvragen correct te beantwoorden.

identiteit
In HP Client Security, een groep referenties en instellingen die worden verwerkt als een account of het profiel voor een bepaalde gebruiker.

ID-kaart
Een gadget op het bureaublad van Windows dat dient om visueel uw bureaublad met uw gebruikersnaam en gekozen afbeelding te identificeren.

Just In Time Authentication
Zie de HP Device Access Manager software Help.

Map Trust Circle
Elke map die door een trust circle wordt beschermd.

nabijheidskaart
Een plastic kaart met een computerchip die gebruikt kan worden voor verificatie in combinatie met andere referenties voor een extra beveiliging.

netwerkaccount

Een Windows-gebruiker of beheerdersaccount, hetzij op een lokale computer, in een werkgroep of op een domein.

noodherstelarchief
Een beveiligd opslaggebied dat het hercoderen mogelijk maakt van basisgebruikerssleutels van één platform eigenaarssleutel naar een andere.

opschonen van vrije ruimte
Het schrijven van willekeurige gegevens over verwijderde gegevenselementen en ongebruikte ruimte. Dit proces vermindert het bestaan van het verwijderde gegevenselement zodat het moeilijker wordt om her originele gegevenselement te herstellen.

opstartverificatie
Een beveiligingsfunctie die een vorm van verificatie vereist, zoals een smartcard, beveiligingschip, of wachtwoord, wanneer de computer wordt ingeschakeld.

Pincode
Een persoonlijk identificatienummer voor een geregistreerde gebruiker, te gebruiken voor verificatie.

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

referentiegegevens
Een specifiek stuk informatie of een hardwareapparaat gebruikt voor de verificatie van een individuele gebruiker.

Single sign-on (Eenmalige aanmelding)
Een functie die informatie over verificatie opslaat en waarmee u HP Client Security kunt gebruiken voor toegang tot Internet en Windows-toepassingen waarvoor wachtwoordverificatie vereist is.

smartcard
Een hardwareapparaat dat met een pincode gebruikt kan worden voor verificatie.

softwarecodering
Het gebruik van software om de vaste schijf sector voor sector te coderen. Dit proces is langzamer dan hardwarecodering

Startpagina
Een centrale locatie waar u de functies en instellingen in HP Client Security kunt bereiken.

toegangsbeleid voor apparaten
De lijst met apparaten waarvoor een gebruiker wel of geen toegang heeft.

Trust Circle
Beveiligt gegevens door deze gegevens te koppelen aan een gedefinieerde groep vertrouwde gebruikers. Dit voorkomt dat gegevens al dan niet opzettelijk in de verkeerde handen vallen. Beveiligd met CryptoMill's Zero Overhead Key Management technologie worden de gegevens cryptografisch gekoppeld aan een vertrouwenskring. Dit voorkomt decodering van documenten of andere gevoelige informatie buiten de trust circle.

Trust Circle Manager/Reader
De Trust Circle Reader kan alleen uitnodigingen accepteren die verzonden zijn door gebruikers van Trust Circle Manager. Maar Trust Circle Manager maakt het mogelijk om trust circles te maken. Functies zijn het per e-mail uitnodigen van iemand tot een trust circle en accepteren van uitnodigingen door anderen. Nadat een trust circle is opgezet, kunnen bestanden die door die trust circle worden beschermd, veilig gedeeld worden.

Trusted Platform Module (TPM) geïntegreerde beveiligingschip
Een TPM verifieert een computer in plaats van een gebruiker, door informatie op te slaan die specifiek is voor het hostsysteem, zoals coderingssleutels, digitale certificaten en wachtwoorden. Een TPM minimaliseert het

risico dat informatie op de computer door fysieke diefstal of door een aanval door een externe hacker wordt gecompromitteerd.

verificatie
Het proces van verificatie dat u de persoon bent die u beweert te zijn, door referenties te gebruiken, inclusief uw Windows-wachtwoord, uw vingerafdruk, een smartcard, een contactloze kaart of een nabijheidskaart.

versleuteling
Een procedure, zoals het gebruik van een algoritme, gebruikt bij cryptografie om platte tekst om te zetten naar gecodeerde tekst om te voorkomen dat ongeoorloofde ontvangers die gegevens kunnen lezen. Er zijn veel soorten gegevenscodering en zij vormen de basis van netwerkbeveiliging. Veel voorkomende typen omvatten Data Encryption Standard en openbare-sleutel codering.

versnipperen
Het uitvoeren van een algoritme dat de gegevens welke zijn opgenomen in een gegevenselement, met betekenisloze gegevens overschrijft.

vingerafdruk
Een digitale extractie van een afbeelding van uw vingerafdruk. De eigenlijke afbeelding van uw vingerafdruk wordt nooit opgeslagen door HP Client Security.

Windows-beheerder
Een gebruiker met alle rechten om machtingen aan te passen en andere gebruikers te beheren.

Windows-gebruikersaccount
Een gebruiker die gerechtigd is om zich aan te melden op een netwerk of op een individuele computer.

Windows Logon beveiliging
Beschermt uw Windows account(s) door het gebruik van specifieke referenties voor toegang te vereisen.

Index