

ProtectTools

Gebruikershandleiding

© Copyright 2007 Hewlett-Packard
Development Company, L.P.

Microsoft en Windows zijn in de Verenigde Staten geregistreerde handelsmerken van Microsoft Corporation. Intel is een handelsmerk of geregistreerd handelsmerk van Intel Corporation of haar dochterbedrijven in de Verenigde Staten en andere landen. AMD, het AMD Arrow-logo en combinaties daarvan zijn handelsmerken van Advanced Micro Devices, Inc. Bluetooth is een handelsmerk van de desbetreffende eigenaar en wordt door Hewlett-Packard Company onder licentie gebruikt. Java is een in de Verenigde Staten geregistreerd handelsmerk van Sun Microsystems, Inc. Het SD-logo is een handelsmerk van de desbetreffende eigenaar.

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

Eerste editie, januari 2007

Artikelnummer van document: 438371-331

Inhoudsopgave

1 Introductie tot beveiliging

Voorzieningen van HP ProtectTools	2
Toegang tot HP ProtectTools Security	4
Belangrijke beveiligingsdoelstellingen realiseren	5
Bescherming bieden tegen gerichte diefstal	5
Toegang tot gevoelige gegevens beperken	5
Ongeoorloofde toegang vanaf interne of externe locaties beperken	6
Beleid met betrekking tot sterke wachtwoorden	6
Extra beveiligingsonderdelen	7
Beveiligingsrollen toewijzen	7
Wachtwoorden van HP ProtectTools beheren	7
Beveiligingswachtwoord instellen	9
HP ProtectTools Backup en herstellen	9
Backup maken van referenties en instellingen	9
Referenties herstellen	11
Instellingen configureren	11

2 Credential Manager for HP ProtectTools

Instelprocedures	14
Credential Manager Logon (Aanmelden bij Credential Manager)	14
Wizard Credential Manager Logon (Aanmelden bij Credential Manager)	
gebruiken	14
Eerste keer aanmelden	15
Referenties registreren	15
Vingerafdrukken vastleggen	15
Vingerafdrukkezer instellen	15
Uw vastgelegde vingerafdruk gebruiken om u aan te melden bij	
Windows	15
Java Card, USB-eToken of virtueel token registreren	15
USB-eToken registreren	16
Andere referenties registreren	16
Algemene taken	17
Virtueel token maken	17
Windows-aanmeldingswachtwoord wijzigen	17
Tokenpincode wijzigen	18
Identiteit beheren	18
Identiteit van het systeem verwijderen	18
Computer vergrendelen	18
Aanmelden bij Windows	19

Aanmelden bij Windows met Credential Manager	19
Account toevoegen	19
Account verwijderen	19
Single Sign On gebruiken	20
Nieuwe applicatie registreren	20
Automatische registratie gebruiken	20
Handmatige registratie (slepen en neerzetten)	21
Applicaties en referenties beheren	21
Eigenschappen van applicaties wijzigen	21
Applicaties uit Single Sign On verwijderen	21
Applicatie exporteren	21
Applicatie importeren	22
Referenties wijzigen	22
Applicatiebescherming gebruiken	23
Toegang tot een applicatie beperken	23
Bescherming van een applicatie opheffen	23
Ingestelde beperkingen voor een beschermde applicatie wijzigen	24
Geavanceerde taken (alleen beheerder)	25
Opgeven hoe gebruikers en beheerders zich aanmelden	25
Aangepaste verificatievereisten configureren	25
Eigenschappen van referenties configureren	26
Instellingen van Credential Manager configureren	26
Voorbeeld 1: de pagina “Advanced Settings” (Geavanceerde instellingen) gebruiken om aanmelden bij Windows vanuit Credential Manager mogelijk te maken	27
Voorbeeld 2: de pagina “Advanced Settings” (Geavanceerde instellingen) gebruiken om gebruikersverificatie te vereisen voor Single Sign On	27

3 Embedded Security for HP ProtectTools

Instelprocedures	30
Embedded Security for ProtectTools	30
Geïntegreerde beveiligingschip initialiseren	30
Basisgebruikersaccount instellen	31
Algemene taken	32
Personal Secure Drive (PSD) gebruiken	32
Bestanden en mappen coderen	32
Gecodeerde e-mail versturen en ontvangen	32
Wachtwoord voor de Basic User Key wijzigen	33
Geavanceerde taken	34
Backup maken en herstellen	34
Backups maken	34
Certificeringsgegevens herstellen vanuit het backupbestand	34
Eigenaarswachtwoord wijzigen	34
Gebruikerswachtwoord herstellen	34
Embedded Security in- en uitschakelen	34
Embedded Security blijvend uitschakelen	35
Embedded Security weer inschakelen na blijvend uitschakelen	35
Sleutels migreren met de wizard Migreren	35

4 Java Card Security for HP ProtectTools

Algemene taken	38
Pincode van een Java Card wijzigen	38
Kaartlezer selecteren	38
Geavanceerde taken (alleen beheerders)	39
Pincode toewijzen aan een Java Card	39
Naam toewijzen aan een Java Card	39
Opstartverificatie instellen	40
Opstartverificatie met Java Card inschakelen en een beheerders-Java Card maken	40
Gebruikers-Java Card maken	41
Opstartverificatie met Java Card uitschakelen	41

5 BIOS Configuration for HP ProtectTools

Algemene taken	44
Opstartopties beheren	44
Systeemconfiguratieopties in- en uitschakelen	44
Geavanceerde taken	47
Instellingen Van aanvullende module voor HP ProtectTools beheren	47
Ondersteuning voor opstartverificatie met Smart Card in- en uitschakelen	47
Opstartverificatie via geïntegreerde beveiligingschip in- en uitschakelen	47
Beveiliging van vaste schijf met Automatic DriveLock in- en uitschakelen	48
Wachtwoorden van Computer Setup (Computerinstellingen) beheren	48
Opstartwachtwoord instellen	49
Opstartwachtwoord wijzigen	49
Instelwachtwoord instellen	49
Instelwachtwoord wijzigen	50
Wachtwoordopties instellen	50
Strengere beveiliging in- en uitschakelen	50
Opstartverificatie bij het opnieuw opstarten van Windows in- en uitschakelen	50

6 Device Access Manager for HP ProtectTools

Achtergrondservice starten	54
Eenvoudige configuratie	55
Configuratie van apparaatklassen (geavanceerd)	56
Gebruiker of groep toevoegen	56
Gebruiker of groep verwijderen	56
Gebruiker of groep toegang weigeren	56
Toegang tot een apparaatklasse verlenen aan één gebruiker van een groep	57
Toegang tot een specifiek apparaat verlenen aan één gebruiker van een groep	57

7 Drive Encryption for HP ProtectTools

Coderingsbeheer	60
Gebruikersbeheer	61
Herstel	63

8 Problemen oplossen

Credential Manager for HP ProtectTools	66
Embedded Security for HP ProtectTools	69

Device Access Manager for HP ProtectTools 76

Overige problemen 77

Woordenlijst 81

Index 83

1 Introductie tot beveiliging

HP ProtectTools Security Manager software bevat beveiligingsvoorzieningen die bescherming bieden tegen ongeoorloofde toegang tot uw computer, netwerken en belangrijke gegevens. De verbeterde beveiligingsfunctionaliteit wordt mogelijk gemaakt door de volgende softwaremodules:

- Credential Manager for HP ProtectTools
- Embedded Security for HP ProtectTools
- Java Card Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Device Access Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools

De softwaremodules die beschikbaar zijn voor uw computer kunnen per model verschillen. Embedded Security for HP ProtectTools is bijvoorbeeld alleen beschikbaar voor computers waarop de geïntegreerde beveiligingschip TPM (Trusted Platform Module) is geïnstalleerd.

HP ProtectTools softwaremodules zijn mogelijk vooraf op uw computer geïnstalleerd of geladen, of als downloadoptie beschikbaar op de website van HP. Kijk voor meer informatie op <http://www.hp.com>.



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

Voorzieningen van HP ProtectTools

In de onderstaande tabel vindt u de belangrijkste voorzieningen van de modules van HP ProtectTools.

Module	Belangrijkste voorzieningen
Credential Manager for HP ProtectTools	• Credential Manager is een veilige bewaarplaats voor uw persoonlijke wachtwoord. • Single Sign On onthoudt meerdere wachtwoorden voor verschillende beveiligde websites, applicaties en netwerkbronnen. • Single Sign On biedt aanvullende bescherming doordat hierbij voor de verificatie van een gebruiker combinaties van beveiligingstechnologieën zijn vereist, zoals een Java™ Card en biometrische lezers. • Wachtwoordopslag wordt beschermd door middel van codering. Deze beveiliging kan verder worden aangescherpt door gebruik van een geïntegreerde TPM-beveiligingschip en/of verificatie door middel van een beveiligingsapparaat, zoals Java Cards of een biometrische lezer.
Embedded Security for HP ProtectTools	• Embedded Security maakt gebruik van een geïntegreerde TPM-beveiligingschip (Trusted Platform Module) voor de bescherming tegen ongeoorloofde toegang tot gevoelige gebruikersgegevens of referenties die lokaal op een computer zijn opgeslagen. • Met Embedded Security kunt u een Personal Secure Drive (PSD) maken. Deze persoonlijke schijf eenheid dient om gebruikersgegevens te beveiligen. • Embedded Security ondersteunt applicaties van derden (waaronder Microsoft Outlook en Internet Explorer) voor het uitvoeren van taken die zijn beveiligd met een digitaal certificaat.
Java Card Security for HP ProtectTools	• Java Card Security configureert de HP ProtectTools Java Card om de gebruiker te kunnen verifiëren voordat het besturingssysteem wordt geladen. • Java Card Security configureert afzonderlijke Java Cards voor beheerders en gebruikers.
BIOS Configuration for HP ProtectTools	• BIOS Configuration biedt toegang tot het beheer van het opstartwachtwoord (het gebruikerswachtwoord) of het beheerderswachtwoord. • BIOS Configuration for HP ProtectTools biedt een alternatief voor het BIOS-configuratiehulpprogramma tijdens het opstarten, beter bekend als f10 Setup (Computerinstellingen). • DriveLock is verbeterd met de geïntegreerde beveiligingschip en beschermt de vaste schijf tegen ongeoorloofde toegang, zelfs als deze uit een systeem is verwijderd. De gebruiker hoeft geen extra wachtwoorden te onthouden, afgezien van het gebruikerswachtwoord van de geïntegreerde beveiligingschip.

Module	Belangrijkste voorzieningen
Device Access Manager for HP ProtectTools	• Met Device Access Manager kunnen systeembeheerders de toegangsrechten voor apparaten beheren op basis van gebruikersprofielen. • Device Access Manager voorkomt dat onbevoegden gegevens kunnen verwijderen door externe opslagmedia te gebruiken of vanaf externe media het systeem kunnen infecteren met een virus. • De beheerder kan de toegang tot beschrijfbare apparaten uitschakelen voor bepaalde personen of gebruikersgroepen.
Drive Encryption for HP ProtectTools	• Drive Encryption biedt volledige codering van de vaste schijf. • Voor Drive Encryption is verificatie vóór het opstarten vereist voor het decoderen van en toegang krijgen tot de gegevens.

Toegang tot HP ProtectTools Security

U opent als volgt HP ProtectTools Security vanuit het Configuratiescherm van Windows®:

- ▲ Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.



OPMERKING: Nadat u de Credential Manager heeft geconfigureerd, kunt u HP ProtectTools openen door u direct vanuit het aanmeldscherm van Windows aan te melden bij de module Credential Manager. Raadpleeg "[Aanmelden bij Windows met Credential Manager op pagina 19](#)" voor meer informatie.

Belangrijke beveiligingsdoelstellingen realiseren

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

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

Bescherming bieden tegen gerichte diefstal

Een voorbeeld van dit type incident is de gerichte diefstal van een computer, die vertrouwelijke gegevens en klantinformatie bevat, bij de beveiligingscontrole op een vliegveld. De volgende voorzieningen bieden bescherming tegen gerichte diefstal:

- De verificatievoorziening vóór het opstarten, wanneer ingeschakeld, voorkomt toegang tot het besturingssysteem. Raadpleeg de volgende procedures:
 - [“Ondersteuning voor opstartverificatie met Smart Card in- en uitschakelen op pagina 47”](#)
 - [“Opstartverificatie via geïntegreerde beveiligingschip in- en uitschakelen op pagina 47”](#)
 - [“Naam toewijzen aan een Java Card op pagina 39”](#)
 - [“Drive Encryption for HP ProtectTools op pagina 59”](#)
- DriveLock zorgt ervoor dat geen toegang tot gegevens kan worden verkregen, zelfs niet als de vaste schijf wordt verwijderd en in een onbeveiligd systeem wordt geïnstalleerd. Raadpleeg [“Beveiliging van vaste schijf met Automatic DriveLock in- en uitschakelen op pagina 48”](#).
- De module Embedded Security for HP ProtectTools biedt de voorziening Personal Secure Drive. Met deze voorziening worden gevoelige gegevens gecodeerd om ervoor te zorgen dat deze niet toegankelijk zijn zonder verificatie. Raadpleeg de volgende procedures:
 - Embedded Security [“Instelprocedures op pagina 30”](#)
 - [“Personal Secure Drive \(PSD\) gebruiken op pagina 32”](#)

Toegang tot gevoelige gegevens beperken

Stel, een externe accountant werkt bij u op locatie en heeft toegang gekregen tot de computer om gevoelige financiële gegevens te bekijken. U wilt echter niet dat de accountant de bestanden kan afdrukken of ze kan opslaan op een beschrijfbaar medium, zoals een cd. Met de volgende voorzieningen kunt u toegang tot gegevens beperken:

- Met Device Access Manager for HP ProtectTools kunnen systeembeheerders toegang tot beschrijfbare apparaten beperken, zodat gevoelige informatie niet kan worden afgedrukt of kan worden gekopieerd naar verwijderbare media vanaf de vaste schijf. Raadpleeg [“Configuratie van apparaatklassen \(geavanceerd\) op pagina 56”](#).
- DriveLock zorgt ervoor dat geen toegang tot gegevens kan worden verkregen, zelfs niet als de vaste schijf wordt verwijderd en in een onbeveiligd systeem wordt geïnstalleerd. Raadpleeg [“Beveiliging van vaste schijf met Automatic DriveLock in- en uitschakelen op pagina 48”](#).

Ongeoorloofde toegang vanaf interne of externe locaties beperken

Als vanaf een interne of externe locatie toegang wordt verkregen tot een computer met vertrouwelijke gegevens, kunnen onbevoegden zich mogelijk toegang verschaffen tot netwerkbronnen of financiële gegevens van het bedrijf, een bestuurslid of een R&D-team, of tot vertrouwelijke informatie zoals patiëntendossiers of persoonlijke financiële gegevens. Met de volgende voorzieningen kunt u ongeoorloofde toegang voorkomen:

- De verificatievoorziening vóór het opstarten, wanneer ingeschakeld, voorkomt toegang tot het besturingssysteem. Raadpleeg de volgende procedures:
 - [“Ondersteuning voor opstartverificatie met Smart Card in- en uitschakelen op pagina 47”](#)
 - [“Opstartverificatie via geïntegreerde beveiligingschip in- en uitschakelen op pagina 47”](#)
 - [“Naam toewijzen aan een Java Card op pagina 39”](#)
 - [“Drive Encryption for HP ProtectTools op pagina 59”](#)
- Embedded Security for HP ProtectTools beschermt met behulp van de volgende procedures gevoelige gebruikersgegevens of referenties die lokaal op een computer zijn opgeslagen:
 - Embedded Security [“Instelprocedures op pagina 30”](#)
 - [“Personal Secure Drive \(PSD\) gebruiken op pagina 32”](#)
- Credential Manager for HP ProtectTools gebruikt de volgende procedures om ervoor te zorgen dat onbevoegden geen toegang hebben tot wachtwoorden of applicaties die zijn beveiligd met een wachtwoord:
 - Credential Manager [“Instelprocedures op pagina 14”](#)
 - [“Single Sign On gebruiken op pagina 20”](#)
- Met Device Access Manager for HP ProtectTools kunnen systeembeheerders toegang tot beschrijfbare apparaten beperken, zodat gevoelige informatie niet kan worden gekopieerd vanaf de vaste schijf. Raadpleeg [“Eenvoudige configuratie op pagina 55”](#).
- De voorziening Personal Secure Drive codeert met behulp van de volgende procedures gevoelige gegevens om ervoor te zorgen dat deze niet toegankelijk zijn zonder verificatie:
 - Embedded Security [“Instelprocedures op pagina 30”](#)
 - [“Personal Secure Drive \(PSD\) gebruiken op pagina 32”](#)

Beleid met betrekking tot sterke wachtwoorden

Als het gebruik van sterke wachtwoorden verplicht wordt gesteld is voor tientallen webapplicaties en databases, biedt Credential Manager for HP ProtectTools een beveiligde opslagplaats voor wachtwoorden en het gemak van Single Sign On. Raadpleeg de volgende procedures:

- Credential Manager [“Instelprocedures op pagina 14”](#)
- [“Single Sign On gebruiken op pagina 20”](#)

Embedded Security for HP ProtectTools beveiligt de opslagplaats vervolgens met gebruikersnamen en wachtwoorden. Op die manier kunnen gebruikers meerdere sterke wachtwoorden onderhouden, zonder deze te hoeven opschrijven of onthouden. Raadpleeg Embedded Security [“Instelprocedures op pagina 30”](#).

Extra beveiligingsonderdelen

Beveiligingsrollen toewijzen

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



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

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

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



OPMERKING: Veel van de voorzieningen van HP ProtectTools kunnen door de beveiligingsmanager worden aangepast in overleg met HP. Raadpleeg de HP website <http://www.hp.com> voor meer informatie.

- **Systeembeheerder:** Past de door de beveiligingsmanager gedefinieerde beveiligingsvoorzieningen toe en beheert deze. De systeembeheerder kan sommige voorzieningen ook in- en uitschakelen. Als de beveiligingsmanager bijvoorbeeld heeft besloten om Java Cards te gebruiken, kan de systeembeheerder de Java Card BIOS-beveiligingsmodus inschakelen.
- **Gebruiker:** Gebruikt de beveiligingsvoorzieningen. Als de beveiligingsmanager en systeembeheerder bijvoorbeeld Java Cards hebben ingeschakeld voor het systeem, kan de gebruiker de pincode voor de Java Card instellen en de kaart gebruiken voor verificatiedoeleinden.

Wachtwoorden van HP ProtectTools beheren

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

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

HP ProtectTools wachtwoord	Instellen in deze HP ProtectTools module	Functie
Aanmeldingswachtwoord Credential Manager	Credential Manager	Dit wachtwoord biedt twee opties: • U kunt dit wachtwoord gebruiken om u apart aan te melden bij Credential Manager nadat u bent aangemeld bij Windows. • U kunt dit wachtwoord gebruiken in plaats van het aanmeldproces van Windows, zodat u zich tegelijkertijd bij Windows en Credential Manager kunt aanmelden.

HP ProtectTools wachtwoord	Instellen in deze HP ProtectTools module	Functie
Wachtwoord herstelbestand Credential Manager	Credential Manager, door systeembeheerder	Beveiligt de toegang tot het herstelbestand van Credential Manager.
Basic User Key, wachtwoord  OPMERKING: Ook wel bekend als Embedded Security wachtwoord	Embedded Security	Dit wachtwoord kunt u gebruiken om toegang te krijgen tot voorzieningen van Embedded Security, zoals beveiligde e-mail en codering van bestanden en mappen. Als dit wachtwoord wordt gebruikt voor opstartverificatie, beveiligt het de toegang tot de inhoud van de computer wanneer deze wordt opgestart of opnieuw wordt opgestart of wanneer de hibernationstand wordt beëindigd.
Wachtwoord voor noodhersteltoken  OPMERKING: Ook wel bekend als Emergency Recovery Token Key wachtwoord	Embedded Security, door systeembeheerder	Beschermst de toegang tot het token voor noodherstel. Dit is een backupbestand voor de geïntegreerde beveiligingschip.
Eigenaarswachtwoord	Embedded Security, door systeembeheerder	Beschermst het systeem en de TPM-beveiligingschip tegen ongeoorloofde toegang tot alle eigenaarsfuncties van Embedded Security.
Pincode Java™ Card	Java Card Security	Beschermst de inhoud van de Java Card en verifieert gebruikers ervan. Als de Java Card wordt gebruikt voor opstartverificatie, beschermt de pincode van de Java Card tevens het hulpprogramma Computer Setup (Computerinstellingen) en de inhoud van de computer. Verifieert Gebruikers van Drive Encryption als het Java Card-token is geselecteerd.
Wachtwoord voor Computer Setup (Computerinstellingen)  OPMERKING: Ook wel bekend als BIOS-beheerderswachtwoord of instelwachtwoord	BIOS-configuratie, door systeembeheerder	Beveiligt de toegang tot het hulpprogramma Computer Setup (Computerinstellingen).
Opstartwachtwoord	BIOS Configuration	Beveiligt de toegang tot de inhoud van de computer wanneer deze wordt opgestart of opnieuw wordt opgestart of wanneer de hibernationstand wordt beëindigd.
Windows-aanmeldingswachtwoord	Windows-configuratiescherm	Kan worden gebruikt voor handmatig aanmelden of worden opgeslagen op de Java Card.

Beveiligingswachtwoord instellen

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

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

HP ProtectTools Backup en herstellen

HP ProtectTools Backup en herstellen biedt een handige en snelle manier om een backup te maken van referenties van alle HP ProtectTools modules en deze te herstellen.

Backup maken van referenties en instellingen

U kunt op elk van de volgende manieren een backup maken van referenties:

- Modules van HP ProtectTools selecteren en er een backup van maken met de HP ProtectTools wizard Backup.
- Backup maken van geselecteerde HP ProtectTools modules



OPMERKING: Voordat u deze methode kunt gebruiken, stelt u de backup-opties in.

- Backups plannen



OPMERKING: Voordat u deze methode kunt gebruiken, stelt u de backup-opties in.

HP ProtectTools modules selecteren en er een backup van maken met de HP ProtectTools wizard Backup

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **HP ProtectTools** en vervolgens op **Backup en herstellen**.
3. Klik in het rechterdeelvenster op **Backup Options** (Backup-opties). De HP ProtectTools wizard Backup wordt geopend. Volg de instructies op het scherm om een backup te maken van referenties.

Backup-opties instellen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **HP ProtectTools** en vervolgens op **Backup en herstellen**.
3. Klik in het rechterdeelvenster op **Backup Options** (Backup-opties). De HP ProtectTools wizard Backup wordt geopend.
4. Volg de instructies op het scherm.
5. Nadat u het **Storage File Password** (Wachtwoord opslagbestand) heeft ingesteld en bevestigd, selecteert u **Remember all passwords and authentication values for future automated backups** (Alle wachtwoorden en verificatiewaarden onthouden voor toekomstige automatische backups).
6. Klik op **Save Settings** (Instellingen opslaan) en vervolgens op **Finish** (Voltooien).

Backup maken van geselecteerde HP ProtectTools modules



OPMERKING: Voordat u deze methode kunt gebruiken, stelt u de backup-opties in.

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **HP ProtectTools** en vervolgens op **Backup en herstellen**.
3. Klik in het rechterdeelvenster op **Backup**.

Backups plannen



OPMERKING: Voordat u deze methode kunt gebruiken, stelt u de backup-opties in.

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **HP ProtectTools** en vervolgens op **Backup en herstellen**.
3. Klik in het rechterdeelvenster op **Backups plannen**.
4. Schakel op het tabblad **Task** (Taak) het selectievakje **Enabled** (Ingeschakeld) in, om geplande backups mogelijk te maken.
5. Klik op **Set Password** (Wachtwoord instellen) en typ en bevestig uw wachtwoord in het dialoogvenster **Set Password** (Wachtwoord instellen). Klik op **OK**.
6. Klik op **Apply** (Toepassen). Klik op het tabblad **Schedule** (Plannen). Klik op de pijl **Schedule Task** (Taak plannen) en selecteer hoe vaak u automatisch een backup wilt maken.

7. Gebruik onder **Start time** (Starttijd) de pijlen om de exacte tijd waarop u de backup wilt maken te selecteren.
8. Klik op **Advanced** (Geavanceerd) om een startdatum, een einddatum en standaard taakinstellingen te selecteren. Klik op **Apply** (Toepassen).
9. Klik op **Settings** (Instellingen) en selecteer instellingen voor **Scheduled Task Completed** (Geplande taak voltooid), **Idle Time** (Tijd inactief) en **Power Management** (Energiebeheer).
10. Klik op **Apply** (Toepassen) en vervolgens op **OK** om het dialoogvenster te sluiten.

Referenties herstellen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **HP ProtectTools** en vervolgens op **Backup en herstellen**.
3. Klik in het rechterdeelvenster op **Restore** (Herstellen). De HP ProtectTools wizard Herstellen wordt geopend. Volg de instructies op het scherm.

Instellingen configureren

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **HP ProtectTools** en vervolgens op **Settings** (Instellingen).
3. Selecteer uw instellingen in het rechterdeelvenster en klik op **OK**.

2 Credential Manager for HP ProtectTools

Credential Manager for HP ProtectTools biedt door middel van de volgende beveiligingsvoorzieningen bescherming tegen ongeoorloofde toegang tot uw computer:

- Aanmelden bij Windows op een andere manier dan met een wachtwoord, bijvoorbeeld door middel van een Java Card of een biometrische lezer. Raadpleeg "[Referenties registreren op pagina 15](#)" voor meer informatie.
- Voorziening van Single Sign On, waarmee automatisch referenties voor websites, applicaties en beveiligde netwerkbronnen worden onthouden.
- Ondersteuning voor optionele beveiligingsapparaten, zoals Java Cards en biometrische lezers.
- Ondersteuning voor aanvullende beveiligingsinstellingen, zoals het vereisen van verificatie met een optioneel beveiligingsapparaat om de computer te ontgrendelen.

Instelprocedures

Credential Manager Logon (Aanmelden bij Credential Manager)

Afhankelijk van de configuratie gebruikt u een van de volgende manieren om u aan te melden bij Credential Manager:

- Wizard Credential Manager Logon (Aanmelden bij Credential Manager) (bij voorkeur)
- Pictogram HP ProtectTools Security Manager in het systeemvak
- HP ProtectTools Security Manager



OPMERKING: Als u de prompt Credential Manager Logon in het Windows-aanmeldingsscherm gebruikt om zich aan te melden bij Credential Manager, wordt u tegelijkertijd bij Windows aangemeld.

De eerste keer dat u Credential Manager opent, meldt u zich aan met uw normale Windows-aanmeldingswachtwoord. Er wordt dan automatisch een Credential Manager account gemaakt met uw Windows-aanmeldingsreferenties.

Nadat u bent aangemeld bij Credential Manager kunt u aanvullende referenties registreren, zoals een vingerafdruk of Java Card. Raadpleeg ["Referenties registreren op pagina 15"](#) voor meer informatie.

De volgende keer dat u zich aanmeldt, kunt u het aanmeldingsbeleid selecteren en een combinatie van de geregistreerde referenties gebruiken.

Wizard Credential Manager Logon (Aanmelden bij Credential Manager) gebruiken

Voer de onderstaande stappen uit om u aan te melden bij Credential Manager met de wizard Credential Manager Logon (Aanmelden bij Credential Manager):

1. Open de wizard Credential Manager Logon (Aanmelden bij Credential Manager) op een van de volgende manieren:
 - Vanuit het Windows-aanmeldingsscherm.
 - Vanuit het systeemvak door te dubbelklikken op het pictogram van **HP ProtectTools Security Manager**.
 - Vanuit de pagina "Credential Manager" van ProtectTools Security Manager door te klikken op de koppeling **Log On** (Aanmelden) rechtsboven in het venster.
2. Volg de instructies op het scherm om u aan te melden bij Credential Manager.

Eerste keer aanmelden

Voordat u begint, zorgt u ervoor dat u aangemeld bent bij Windows met een beheerdersaccount, maar niet aangemeld bij Credential Manager.

1. Open HP ProtectTools Security Manager door te dubbelklikken op het pictogram HP ProtectTools Security Manager in het systeemvak. Het venster van de HP ProtectTools Security Manager wordt geopend.
2. Klik in het linkerdeelvenster op **Credential Manager**, en vervolgens op **Log On** (Aanmelden) in de linkerbovenhoek van het rechterdeelvenster. De wizard Credential Manager Logon (Aanmelden bij Credential Manager) wordt geopend.
3. Typ uw Windows-wachtwoord in het vak **User name** (Gebruikersnaam) en klik op **Next** (Volgende).

Referenties registreren

Op de pagina "My Identity" (Mijn identiteit) kunt u uw verschillende verificatiemethoden of referenties registreren. Nadat deze zijn geregistreerd, kunt u de methoden gebruiken voor aanmelding bij Credential Manager.

Vingerafdrukken vastleggen

Met een vingerafdrukkezer kunt u zich bij Windows aanmelden met uw vingerafdruk, in plaats van een Windows-wachtwoord.

Vingerafdrukkezer instellen

1. Nadat u zich heeft aangemeld bij Credential Manager, haalt u uw vinger over de vingerafdrukkezer. De wizard Credential Manager Logon (Aanmelden bij Credential Manager) wordt geopend.
2. Volg de instructies op het scherm om uw vingerafdrukken te registreren en de vingerafdrukkezer in te stellen.
3. Als u de vingerafdrukkezer wilt instellen voor een andere gebruiker van Windows, meldt u zich bij Windows aan als de desbetreffende gebruiker en herhaalt u stap 1 en 2.

Uw vastgelegde vingerafdruk gebruiken om u aan te melden bij Windows

1. Meteen nadat u uw vingerafdrukken heeft vastgelegd, start u Windows opnieuw.
2. Haal een van uw vingers waarvan de afdruk is geregistreerd langs de sensor wanneer het welkomsscherm van Windows verschijnt, om u aan te melden bij Windows.

Java Card, USB-eToken of virtueel token registreren



OPMERKING: Voor deze procedures moet een kaartlezer zijn geconfigureerd. Als u geen lezer heeft geïnstalleerd, kunt u een virtueel token registreren zoals beschreven in "[Virtueel token maken op pagina 17.](#)"

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager**.

3. Klik in het rechterdeelvenster op **Register Smart Card or Token** (Smart Card of token registreren). De wizard Credential Manager Logon (Aanmelden bij Credential Manager) wordt geopend.
4. Volg de instructies op het scherm.

USB-eToken registreren

1. Zorg ervoor dat de stuurprogramma's voor het USB-eToken zijn geïnstalleerd.



OPMERKING: Raadpleeg de gebruikershandleiding van het USB-eToken voor meer informatie.

2. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
3. Klik in het linkerdeelvenster op **Credential Manager**.
4. Klik in het rechterdeelvenster op **Register Smart Card or Token** (Smart Card of token registreren). De wizard Credential Manager Logon (Aanmelden bij Credential Manager) wordt geopend.
5. Volg de instructies op het scherm.

Andere referenties registreren

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager**.
3. Klik in het rechterdeelvenster op **Register Credentials** (Referenties registreren). De wizard Credential Manager Logon (Aanmelden bij Credential Manager) wordt geopend.
4. Volg de instructies op het scherm.

Algemene taken

Alle gebruikers hebben toegang tot de pagina “My Identity” (Mijn identiteit) in Credential Manager. Vanaf deze pagina kunt u de volgende taken uitvoeren:

- Virtueel token maken
- Windows-aanmeldingswachtwoord wijzigen
- Tokenpincode beheren
- Identiteit beheren
- Computer vergrendelen



OPMERKING: Deze optie is alleen beschikbaar als de klassieke aanmeldprompt is ingeschakeld voor Credential Manager. Raadpleeg [“Voorbeeld 1: de pagina “Advanced Settings” \(Geavanceerde instellingen\) gebruiken om aanmelden bij Windows vanuit Credential Manager mogelijk te maken op pagina 27”](#).

Virtueel token maken

Een virtueel token werkt ongeveer op dezelfde manier als een Java Card of een USB-eToken. Het token wordt opgeslagen op de vaste schijf van de computer of in het register van Windows. Wanneer u zich aanmeldt met een virtueel token, wordt u om een gebruikerspincode gevraagd om de verificatie te voltooien.

U maakt een virtueel token als volgt:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager**.
3. Klik in het rechterdeelvenster op **Virtual Token** (Virtueel token). De wizard Credential Manager Logon (Aanmelden bij Credential Manager) wordt geopend.



OPMERKING: Als **Virtual Token** (Virtueel token) geen optie is, gebruikt u de procedure [“Andere referenties registreren op pagina 16.”](#)

4. Volg de instructies op het scherm.

Windows-aanmeldingswachtwoord wijzigen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager**.
3. Klik in het rechterdeelvenster op **Change Windows Password** (Windows-wachtwoord wijzigen).
4. Typ uw oude wachtwoord in het vak **Old password** (Oud wachtwoord).
5. Typ uw nieuwe wachtwoord in de vakken **New password** (Nieuw wachtwoord) en **Confirm password** (Wachtwoord bevestigen).
6. Klik op **Finish** (Voltooien).

Tokenpincode wijzigen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager**.
3. Klik in het rechterdeelvenster op **Change Token PIN** (Tokenpincode wijzigen).
4. Selecteer het token waarvoor u de pincode wilt wijzigen en klik op **Next** (Volgende).
5. Volg de instructies op het scherm om het wijzigen van de pincode te voltooien.

Identiteit beheren

Identiteit van het systeem verwijderen



OPMERKING: Dit heeft geen invloed op uw Windows-gebruikersaccount.

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager**.
3. Klik in het rechterdeelvenster op **Clear Identity for this account** (Identiteit voor deze account wissen).
4. Klik op **Yes** (Ja) in het dialoogvenster dat wordt geopend. Uw identiteit wordt afgemeld en van het systeem verwijderd.

Computer vergrendelen

Deze voorziening is beschikbaar als u zich aanmeldt bij Windows via Credential Manager. Als u uw computer wilt beveiligen wanneer u niet achter uw bureau zit, gebruikt u de functie Lock Workstation (Werkstation vergrendelen). Hierdoor kunnen onbevoegden geen toegang krijgen tot uw computer. Alleen uzelf en leden van de groep Administrators op uw computer kunnen deze ontgrendelen.



OPMERKING: Deze optie is alleen beschikbaar als de klassieke aanmeldprompt is ingeschakeld voor Credential Manager. Raadpleeg "[Voorbeeld 1: de pagina 'Advanced Settings' \(Geavanceerde instellingen\) gebruiken om aanmelden bij Windows vanuit Credential Manager mogelijk te maken op pagina 27](#)".

Voor extra beveiliging kunt u de voorziening Lock Workstation (Werkstation vergrendelen) zo configureren dat een Java Card, biometrische lezer of token vereist is om de computer te ontgrendelen. Raadpleeg "[Instellingen van Credential Manager configureren op pagina 26](#)" voor meer informatie.

U vergrendelt de computer als volgt:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager**.
3. Klik in het rechterdeelvenster op **Lock Workstation** (Werkstation vergrendelen). Het Windows-aanmeldingsscherm verschijnt. U heeft een Windows-wachtwoord of de wizard Credential Manager Logon (Aanmelden bij Credential Manager) nodig om de computer te kunnen vergrendelen.

Aanmelden bij Windows

U kunt Credential Manager gebruiken om u aan te melden bij Windows, hetzij op een lokale computer, hetzij in een netwerkdomrein. Wanneer u zich de eerste keer aanmeldt bij Credential Manager, wordt uw lokale Windows-gebruikersaccount automatisch toegevoegd als account voor aanmelden bij Windows.

Aanmelden bij Windows met Credential Manager

U kunt Credential Manager gebruiken om u aan te melden bij een Windows-netwerk of een lokale account.

1. Als u uw vingerafdruk heeft vastgelegd zodat u zich ermee kunt aanmelden bij Windows, veegt u uw vinger langs de sensor om u aan te melden.
2. Als u uw vingerafdruk niet heeft vastgelegd zodat u zich ermee kunt aanmelden bij Windows, klikt u op het toetsenbordpictogram in de linkerbovenhoek van het scherm, naast het pictogram van de vingerafdruk. De wizard Credential Manager Logon (Aanmelden bij Credential Manager) wordt geopend.
3. Klik op de pijl bij **User name** (Gebruikersnaam) en selecteer uw naam.
4. Typ uw Windows-wachtwoord in het vak **Password** (Wachtwoord) en klik op **Next** (Volgende).
5. Selecteer **More > Wizard Options** (Meer > Wizard-opties).
 - a. Als u wilt dat dit de standaardgebruikersnaam is wanneer u zich de volgende keer aanmeldt bij de computer, schakelt u het selectievakje **Use last user name on next logon** (Gebruik laatste gebruikersnaam bij volgende aanmelding) in.
 - b. Als u wilt dat deze aanmeldprocedure de standaardprocedure is, schakelt u het selectievakje **Use this policy next time you log on** (Deze procedure gebruiken wanneer u zich de volgende keer aanmeldt) in.
6. Volg de instructies op het scherm. Als uw referenties juist zijn, wordt u aangemeld bij uw Windows-account en bij Credential Manager.

Account toevoegen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Services and Applications** (Mijn services en applicaties).
3. Klik in het rechterdeelvenster op **Windows Logon** (Windows-aanmelding) en klik vervolgens op **Add a Network Account** (Netwerkkaccount toevoegen). De wizard Add Network Account (Netwerkkaccount toevoegen) wordt geopend.
4. Volg de instructies op het scherm.

Account verwijderen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Services and Applications** (Mijn services en applicaties).

3. Klik in het rechterdeelvenster op **Windows Logon** (Windows-aanmelding) en klik vervolgens op **Manage Network Accounts** (Netwerkkaccounts beheren). Het dialoogvenster **Manage Network Accounts** (Netwerkkaccounts beheren) wordt geopend.
4. Klik op de account die u wilt verwijderen en klik op **Remove** (Verwijderen).
5. Klik op **Yes** (Ja) in het dialoogvenster dat wordt geopend.
6. Klik op **OK**.

Single Sign On gebruiken

Credential Manager beschikt over een Single Sign On voorziening, waarmee gebruikersnamen en wachtwoorden voor meerdere internet- en Windows-programma's worden opgeslagen en referenties automatisch worden ingevoerd wanneer u een geregistreerd programma opent.



OPMERKING: Veiligheid en privacy zijn belangrijke eigenschappen van Single Sign On. Alle referenties worden gecodeerd en zijn alleen beschikbaar na aanmelding bij Credential Manager.

OPMERKING: U kunt Single Sign On ook zo configureren dat uw verificatiereferenties worden gevalideerd met een Java Card, een vingerafdruklezer of een token voordat u zich aanmeldt bij een beveiligde website of beveiligd programma. Dit komt met name van pas bij het aanmelden bij programma's of websites die persoonlijke gegevens bevatten, zoals bankrekeningnummers. Raadpleeg "[Instellingen van Credential Manager configureren op pagina 26](#)" voor meer informatie.

Nieuwe applicatie registreren

Credential Manager vraagt om applicaties te registreren die u start terwijl u bij Credential Manager bent aangemeld. U kunt een applicatie ook handmatig registreren.

Automatische registratie gebruiken

1. Open een applicatie die aanmelding vereist.
2. Klik op het pictogram Credential Manager SSO in het dialoogvenster waarin u uw wachtwoord voor het programma of de website moet invoeren.
3. Voer uw wachtwoord in voor het programma of de website en klik op **OK**. Het dialoogvenster **Credential Manager Single Sign On** wordt geopend.
4. Klik op **More** (Meer) en selecteer een van de volgende opties:
 - Do not use SSO for this site or application (Gebruik SSO niet voor deze site of applicatie).
 - Prompt to select account for this application (Geef prompt weer om account voor deze applicatie te selecteren).
 - Fill in credentials but do not submit (Referenties invoeren, maar niet verzenden).
 - Authenticate user before submitting credentials (Gebruiker verifiëren alvorens referenties te verzenden).
 - Show SSO shortcut for this application (Toon SSO-shortcut voor deze applicatie).
5. Klik op **Yes** (Ja) om de registratie te voltooien.

Handmatige registratie (slepen en neerzetten)

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Services and Applications** (Mijn services en applicaties).
3. Klik in het rechterdeelvenster op **Single Sign On** en klik vervolgens op **Register New Application** (Nieuwe applicatie registreren). De wizard SSO Application (SSO-applicatie) wordt geopend.
4. Volg de instructies op het scherm.

Applicaties en referenties beheren

Eigenschappen van applicaties wijzigen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Services and Applications** (Mijn services en applicaties).
3. Klik in het rechterdeelvenster onder **Single Sign On** op **Manage Applications and Credentials** (Applicaties en referenties beheren).
4. Klik op de applicatie die u wilt wijzigen en vervolgens op **Properties** (Eigenschappen).
5. Klik op het tabblad **General** (Algemeen) om de naam en de beschrijving van de applicatie te wijzigen. Wijzig de instellingen door de selectievakjes naast de desbetreffende instellingen in of uit te schakelen.
6. Klik op het tabblad **Script** om het SSO-applicatiescript weer te geven en te bewerken.
7. Klik op **OK**.

Applicaties uit Single Sign On verwijderen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Services and Applications** (Mijn services en applicaties).
3. Klik in het rechterdeelvenster onder **Single Sign On** op **Manage Applications and Credentials** (Applicaties en referenties beheren).
4. Klik op de applicatie die u wilt verwijderen en vervolgens op **Remove** (Verwijderen).
5. Klik op **Yes** (Ja) in het dialoogvenster dat wordt geopend.
6. Klik op **OK**.

Applicatie exporteren

U kunt applicaties exporteren om een kopie (backup) te maken van het SSO-applicatiescript. Dit bestand kunt u vervolgens gebruiken om de SSO-gegevens te herstellen. De gegevens fungeren als aanvulling op het backupbestand van de identiteit, dat alleen de referentiegegevens bevat.

U exporteert een applicatie als volgt:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Services and Applications** (Mijn services en applicaties).
3. Klik in het rechterdeelvenster onder **Single Sign On** op **Manage Applications and Credentials** (Applicaties en referenties beheren).
4. Klik op de applicatie die u wilt exporteren. Klik vervolgens op **More (Meer) > Applications** (Applicaties) > **Export Script** (Script exporteren).
5. Volg de instructies op het scherm om het exporteren te voltooien.
6. Klik op **OK**.

Applicatie importeren

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Services and Applications** (Mijn services en applicaties).
3. Klik in het rechterdeelvenster onder **Single Sign On** op **Manage Applications and Credentials** (Applicaties en referenties beheren).
4. Klik op de applicatie die u wilt importeren. Klik vervolgens op **More (Meer) > Applications** (Applicaties) > **Import Script** (Script importeren).
5. Volg de instructies op het scherm om het importeren te voltooien.
6. Klik op **OK**.

Referenties wijzigen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Services and Applications** (Mijn services en applicaties).
3. Klik in het rechterdeelvenster onder **Single Sign On** op **Manage Applications and Credentials** (Applicaties en referenties beheren).
4. Klik op de applicatie die u wilt wijzigen en vervolgens op **More (Meer)**.
5. Selecteer een van de volgende opties:
 - Applications (Applicaties)
 - Add New (Nieuwe toevoegen)
 - Remove (Verwijderen)
 - Properties (Eigenschappen)

- Import Script (Script importeren)
- Export Script (Script exporteren)
- Referenties
 - Create New (Nieuwe aanmaken)
- View Password (Wachtwoord bekijken)



OPMERKING: Verifieer uw identiteit voordat u het wachtwoord bekijkt.

6. Volg de instructies op het scherm.
7. Klik op **OK**.

Applicatiebescherming gebruiken

Met deze voorziening kunt u de toegang tot applicaties configureren. U kunt toegang beperken op basis van de volgende criteria:

- Gebruikerscategorie
- Gebruikstijd
- Inactiviteit gebruiker

Toegang tot een applicatie beperken

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Services and Applications** (Mijn services en applicaties).
3. Klik in het rechterdeelvenster onder **Application Protection** (Applicatiebescherming) op **Manage Protected Applications** (Beschermdde applicaties beheren). Het dialoogvenster **Application Protection Service** (Applicatiebeschermingservice) wordt geopend.
4. Selecteer een categorie gebruiker waarvoor u de toegang wilt beheren.



OPMERKING: Als de categorie niet Everyone (Iedereen) is, kan het noodzakelijk zijn om **Override default settings** (Voorbijgaan aan standaardinstellingen) te selecteren om voorbij te gaan aan de instellingen voor de categorie Everyone (Iedereen).

5. Klik op **Toevoegen**. De wizard Add a Program (Programma toevoegen) wordt geopend.
6. Volg de instructies op het scherm.

Bescherming van een applicatie opheffen

U heft als volgt de beperkingen van een applicatie op:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Services and Applications** (Mijn services en applicaties).

3. Klik in het rechterdeelvenster onder **Application Protection** (Applicatiebescherming) op **Manage Protected Applications** (Beschermdes applicaties beheren). Het dialoogvenster **Application Protection Service** (Applicatiebeschermingservice) wordt geopend.
 4. Selecteer een categorie gebruiker waarvoor u de toegang wilt beheren.
-
-  **OPMERKING:** Als de categorie niet Everyone (Iedereen) is, kan het noodzakelijke zijn om **Override default settings** (Voorbijgaan aan standaardinstellingen) te selecteren om voorbij te gaan aan de instellingen voor de categorie Everyone (Iedereen).
-
5. Klik op de applicatie die u wilt verwijderen en vervolgens op **Remove** (Verwijderen).
 6. Klik op **OK**.

Ingestelde beperkingen voor een beschermde applicatie wijzigen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
 2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Services and Applications** (Mijn services en applicaties).
 3. Klik in het rechterdeelvenster onder **Application Protection** (Applicatiebescherming) op **Manage Protected Applications** (Beschermdes applicaties beheren). Het dialoogvenster **Application Protection Service** (Applicatiebeschermingservice) wordt geopend.
 4. Selecteer een categorie gebruiker waarvoor u de toegang wilt beheren.
-
-  **OPMERKING:** Als de categorie niet Everyone (Iedereen) is, kunt u **Override default settings** (Voorbijgaan aan standaardinstellingen) selecteren om voorbij te gaan aan de instellingen voor de categorie Everyone (Iedereen).
-
5. Klik op de applicatie die u wilt wijzigen en klik op **Properties** (Eigenschappen). Het dialoogvenster **Properties** (Eigenschappen) wordt geopend voor die applicatie.
 6. Klik op het tabblad **General** (Algemeen). Selecteer een van de volgende instellingen:
 - Disabled (Cannot be used) (Uitgeschakeld (Kan niet worden gebruikt))
 - Enabled (Can be used without restrictions) (Ingeschakeld (Kan zonder beperkingen worden gebruikt))
 - Restricted (Usage depends on settings) (Beperkt (Gebruik is afhankelijk van de instellingen))
 7. Wanneer u Restricted (Beperkt) selecteert, zijn de volgende opties beschikbaar:
 - a. Als u gebruik wil beperken op basis van tijd, dag, of datum, klikt u op het tabblad **Schedule** (Planning) en configureert u de instellingen.
 - b. Als u gebruik wilt beperken op basis van inactiviteit, klikt u op het tabblad **Advanced** (Geavanceerd) en selecteert u de periode van inactiviteit.
 8. Klik op **OK** om het dialoogvenster **Properties** (Eigenschappen) van de applicatie te sluiten.
 9. Klik op **OK**.

Geavanceerde taken (alleen beheerder)

De pagina's "Authentication and Credentials" (Verificatie en referenties) en "Advanced Settings" (Geavanceerde instellingen) van Credential Manager zijn alleen beschikbaar voor gebruikers met beheerdersrechten. Vanaf deze pagina's kunt u de volgende taken uitvoeren:

- Opgeven hoe gebruikers en beheerders zich aanmelden
- Aangepaste verificatievereisten configureren
- Eigenschappen van referenties configureren
- Instellingen van Credential Manager configureren

Opgeven hoe gebruikers en beheerders zich aanmelden

Op de pagina "Authentication and Credentials" (Verificatie en referenties) kunt u opgeven welk type referentie of welke combinatie van referenties vereist is voor gebruikers of beheerders.

U geeft als volgt op hoe gebruikers en beheerders zich aanmelden:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Authentication and Credentials** (Verificatie en referenties).
3. Klik in het rechterdeelvenster op het tabblad **Authentication** (Verificatie).
4. Klik op de categorie (**Users** (Gebruikers) of **Administrators** (Beheerders)) in de lijst met categorieën.
5. Klik in de lijst op het type verificatiemethode of een combinatie van methoden.
6. Klik op **Apply** (Toepassen) en vervolgens op **OK**.

Aangepaste verificatievereisten configureren

Als de set verificatiereferenties die u wilt gebruiken niet op het tabblad Authentication (Verificatie) van de pagina "Authentication and Credentials" (Verificatie en referenties) voorkomt, kunt u aangepaste vereisten maken.

U configureert als volgt aangepaste vereisten:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Authentication and Credentials** (Verificatie en referenties).
3. Klik in het rechterdeelvenster op het tabblad **Authentication** (Verificatie).
4. Klik op de categorie (**Users** (Gebruikers) of **Administrators** (Beheerders)) in de lijst met categorieën.
5. Klik op **Custom** (Aangepast) in de lijst met verificatiemethoden.
6. Klik op **Configure** (Configureren).
7. Selecteer de verificatiemethoden die u wilt gebruiken.

8. Kies de combinatie van methoden door op een van de volgende opties te klikken:
 - Gebruik **AND (EN)** om de verificatiemethoden te combineren.
(Gebruikers moeten telkens wanneer ze zich aanmelden alle verificatiemethoden gebruiken die u heeft ingeschakeld.)
 - Gebruik **OR (OF)** om een van twee of meer verificatiemethoden verplicht te stellen
(Gebruikers kunnen, telkens wanneer ze zich aanmelden, een van de geselecteerde methoden kiezen.)
9. Klik op **OK**.
10. Klik op **Apply** (Toepassen) en vervolgens op **OK**.

Eigenschappen van referenties configureren

Op het tabblad **Credentials** (Referenties) van de pagina “Authentication and Credentials” (Verificatie en referenties) kunt u de lijst van beschikbare verificatiemethoden bekijken en de instellingen wijzigen.

U configureert de referenties als volgt:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Authentication and Credentials** (Verificatie en referenties).
3. Klik in het rechterdeelvenster op het tabblad **Credentials** (Referenties).
4. Klik op de referentie die u wilt wijzigen. U kunt de referentie wijzigen op een van de volgende manieren:
 - Registreer de referentie door op **Register** (Registreren) te klikken en volg de instructies op het scherm.
 - Als u de referentie wilt verwijderen, klikt u op **Clear** (Wissen) en vervolgens op **Yes** (Ja) in het dialoogvenster dat wordt geopend.
 - Als u de eigenschappen van de referentie wilt wijzigen, klikt u op **Properties** (Eigenschappen) en volgt u de instructies op het scherm.
5. Klik op **Apply** (Toepassen) en vervolgens op **OK**.

Instellingen van Credential Manager configureren

Vanaf de pagina “Settings” (Instellingen) kunt u verschillende instellingen bekijken en wijzigen op de volgende tabbladen:

- **General** (Algemeen): hiermee kunt u de instellingen voor de basisconfiguratie wijzigen.
- **Single Sign On**: hiermee kunt u de instellingen voor de werking van Single Sign On voor de huidige gebruiker wijzigen, zoals de manier waarop wordt omgegaan met gevonden aanmeldingsschermen, automatisch aanmelden bij geregistreerde aanmelddialoogvensters en weergave van wachtwoorden.
- **Services and Applications** (Mijn services en applicaties): hiermee kunt u de beschikbare services bekijken en de instellingen voor die services wijzigen.

- Security (Beveiliging): hiermee kunt u de software van de vingerafdruklezer selecteren en het beveiligingsniveau van de vingerafdruklezer aanpassen.
- Smart Cards and Tokens (Smart Cards en tokens): hiermee kunt u de eigenschappen voor alle beschikbare Java Cards en tokens bekijken en wijzigen.

U wijzigt instellingen van Credential Manager als volgt:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Settings** (Instellingen).
3. Klik in het rechterdeelvenster op het juiste tabblad voor de instellingen die u wilt wijzigen.
4. Volg de instructies op het scherm om de instellingen te wijzigen.
5. Klik op **Apply** (Toepassen) en vervolgens op **OK**.

Voorbeeld 1: de pagina “Advanced Settings” (Geavanceerde instellingen) gebruiken om aanmelden bij Windows vanuit Credential Manager mogelijk te maken

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Settings** (Instellingen).
3. Klik in het rechterdeelvenster op het tabblad **General** (Algemeen).
4. Schakel onder **Select the way users log on to Windows (requires restart)** (Selecteer de manier waarop gebruikers zich aanmelden bij Windows (opnieuw opstarten vereist)) het selectievakje **Use Credential Manager with classic logon prompt** (Gebruik Credential Manager met klassieke aanmeldprompt) in.
5. Klik op **Apply** (Toepassen) en vervolgens op **OK**.
6. Start de computer opnieuw op.



OPMERKING: Als het selectievakje **Use Credential Manager with classic logon prompt** (Gebruik Credential Manager met klassieke aanmeldprompt) is ingeschakeld, kunt u uw computer vergrendelen. Raadpleeg “[Computer vergrendelen op pagina 18](#)”.

Voorbeeld 2: de pagina “Advanced Settings” (Geavanceerde instellingen) gebruiken om gebruikersverificatie te vereisen voor Single Sign On

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Credential Manager** en vervolgens op **Settings** (Instellingen).
3. Klik in het rechterdeelvenster op het tabblad **Single Sign On**.
4. Schakel onder **When registered logon dialog or Web page is visited** (Bij bezoek aan geregistreerd aanmeldingsdialoogvenster of geregistreerde webpagina) het selectievakje **Authenticate user before submitting credentials** (Gebruiker verifiëren voor verzending van referenties) in.
5. Klik op **Apply** (Toepassen) en vervolgens op **OK**.
6. Start de computer opnieuw op.

3 Embedded Security for HP ProtectTools



OPMERKING: De optionele geïntegreerde beveiligingschip TPM (TPM = Trusted Platform Module) moet in de computer zijn geïnstalleerd om Embedded Security for HP ProtectTools te kunnen gebruiken.

Embedded Security for HP ProtectTools biedt bescherming tegen ongeoorloofde toegang tot gegevens of referenties van de gebruiker. Deze softwaremodule biedt de volgende beveiligingsvoorzieningen:

- Enhanced Microsoft® Encryption File System (EFS) voor het coderen van bestanden en mappen
- Personal Secure Drive (PSD) maken voor het beschermen van gebruikersgegevens
- Gegevensbeheerfuncties, zoals het maken van backups en het herstellen van de sleutelhiërarchie
- Ondersteuning voor toepassingen van derden (waaronder Microsoft Outlook en Internet Explorer) voor het uitvoeren van taken die zijn beveiligd met een digitaal certificaat bij gebruik van de geïntegreerde beveiligingssoftware

De geïntegreerde TPM-beveiligingschip verbetert de beveiligingsvoorzieningen van HP ProtectTools Security Manager en is voor sommige daarvan onmisbaar. Zo kan Credential Manager for HP ProtectTools bijvoorbeeld de chip als verificatiefactor gebruiken wanneer de gebruiker zich aanmeldt bij Windows. Op bepaalde modellen maakt de optionele geïntegreerde TPM-beveiligingschip verbeterde BIOS-beveiligingsfuncties mogelijk die beschikbaar zijn via BIOS Configuration for HP ProtectTools.

Instelprocedures



VOORZICHTIG: Als u beveiligingsrisico's wilt verlagen, is het van belang dat uw systeembeheerder de geïntegreerde beveiligingschip direct initialiseert. Als de geïntegreerde beveiligingschip niet wordt geïnitieerd, kan een ongeautoriseerde gebruiker, een computerworm of een virus mogelijk de computer of de zeggenschap over de taken van de eigenaar overnemen, zoals het beheer van het archief voor noodherstel en het configureren van de toegangsinstellingen voor gebruikers.

Volg de stappen in de volgende twee gedeelten om de geïntegreerde beveiligingschip in te schakelen en te initialiseren.

Embedded Security for ProtectTools

De geïntegreerde beveiligingschip kunt u inschakelen in het hulpprogramma Computer Setup (Computerinstellingen). Deze procedure kan niet worden uitgevoerd in BIOS Configuration for HP ProtectTools.

U schakelt als volgt de geïntegreerde beveiligingschip in:

1. Open Computer Setup (Computerinstellingen) door de computer aan te zetten of opnieuw te starten en op **f10** te drukken wanneer het bericht "f10 = ROM Based Setup" (f10 = ROM-hulpprogramma instellingen) linksonder op het scherm verschijnt.
2. Als u nog geen beheerderswachtwoord heeft ingesteld, selecteert u **Beveiliging > Instelwachtwoord** met behulp van de pijltoetsen, en drukt u vervolgens op **enter**.
3. Typ het wachtwoord in de velden **Nieuw wachtwoord** en **Nieuw wachtwoord bevestigen** en druk op **f10**.
4. Selecteer in het menu **Beveiliging** met de pijltoetsen **TPM geïntegreerde beveiliging** en druk op **enter**.
5. Als het apparaat verborgen is, selecteert u **Available** (Beschikbaar) onder **Embedded Security**.
6. Selecteer **Embedded security device state** (Status geïntegreerd apparaat) en stel deze in op **Enable** (Inschakelen).
7. Druk op **f10** om de gewijzigde instellingen in Embedded Security te accepteren.
8. Selecteer met de pijltoetsen **Bestand > Wijzigingen opslaan en afsluiten** om uw voorkeuren op te slaan en Computer Setup (Computerinstellingen) af te sluiten. Volg daarna de instructies op het scherm.

Geïntegreerde beveiligingschip initialiseren

Tijdens de initialisatieprocedure voor Embedded Security doet u het volgende:

- Een eigenaarswachtwoord instellen voor de geïntegreerde beveiligingschip. Dit wachtwoord beschermt de toegang tot alle eigenaarsfuncties van de geïntegreerde beveiligingschip beschermt.
- Het archief voor noodherstel instellen. Dit is een beveiligde opslagruimte waarmee voor alle gebruikers de Basic User Keys opnieuw kunnen worden gecodeerd.

U initialiseert de geïntegreerde beveiligingschip als volgt:

1. Klik met de rechtermuisknop op het pictogram van de HP ProtectTools Security Manager in het systeemvak aan de rechterkant van de taakbalk en selecteer **Embedded Security Initialization** (Embedded Security initialiseren).

De wizard HP ProtectTools Embedded Security Initialization (Embedded Security initialiseren) wordt geopend.

2. Volg de instructies op het scherm.

Basisgebruikersaccount instellen

Nadat u de basisgebruikersaccount heeft ingesteld, kunt u de volgende taken uitvoeren:

- Een Basic User Key aanmaken die gecodeerde informatie beschermt en een wachtwoord instellen voor de Basic User Key waarmee deze wordt beveiligd.
- Een personal secure drive (PSD) instellen waarop u gecodeerde bestanden en mappen kunt opslaan.



VOORZICHTIG: Berg het wachtwoord voor de Basic User Key op een veilige plaats op. Gecodeerde informatie is niet toegankelijk en kan niet worden hersteld zonder dit wachtwoord.

Ga als volgt te werk om een basisgebruikersaccount in te stellen en de beveiligingsvoorzieningen voor de gebruiker in te schakelen:

1. Als de wizard Embedded Security User Initialization nog niet is geopend, selecteert u **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Geïntegreerde beveiliging** en vervolgens op **Beveiliging**.
3. Klik in het rechterdeelvenster onder **Embedded Security Features** (Voorzieningen Embedded Security) op **Configure** (Configureren).

De wizard Embedded Security User Initialization wordt geopend.

4. Volg de instructies op het scherm.



OPMERKING: Als u de beveiligde e-mail wilt gebruiken, configureert u eerst de e-mailclient zodat deze een digitaal certificaat gebruikt dat is aangemaakt met Embedded Security. Als geen digitaal certificaat beschikbaar is, kunt u deze aanschaffen bij instanties die deze certificaten verstrekken. Raadpleeg de online Help van de e-mailclient voor instructies voor het configureren van uw e-mail en het verkrijgen van een digitaal certificaat.

Algemene taken

Nadat u de basisgebruikersaccount heeft ingesteld, kunt u de volgende taken uitvoeren:

- Bestanden en mappen coderen
- Gecodeerde e-mail versturen en ontvangen

Personal Secure Drive (PSD) gebruiken

Nadat u de PSD heeft ingesteld, wordt u de volgende keer dat u zich aanmeldt gevraagd het wachtwoord voor de Basic User Key in te voeren. Als het juiste wachtwoord invoert voor de Basic User Key, heeft u rechtstreeks toegang tot de PSD vanuit Windows Verkenner.

Bestanden en mappen coderen

Neem de volgende richtlijnen in acht als u met de gecodeerde bestanden werkt:

- Alleen bestanden en mappen op NTFS-partities kunnen worden gecodeerd. Bestanden en mappen op FAT-partities kunnen niet worden gecodeerd.
- Systeembestanden en gecomprimeerde bestanden kunnen niet worden gecodeerd, en gecodeerde bestanden kunnen niet worden gecomprimeerd.
- Zorg ervoor dat tijdelijke mappen gecodeerd zijn, aangezien deze mogelijk interessant zijn voor hackers.
- Wanneer u voor de eerste keer een bestand of map codeert, wordt automatisch een herstelbeleid ingesteld. Dankzij dit beleid kunt u uw informatie decoderen met behulp van een herstelagent als u uw coderingscertificaten en privésleutels mocht verliezen.

U codeert als volgt bestanden en mappen:

1. Klik met uw rechtermuisknop op het bestand of de map om te coderen.
2. Klik op **Encrypt** (Coderen).
3. Selecteer een van de volgende opties:
 - **Apply changes to this folder only** (Wijzigingen alleen op deze map toepassen)
 - **Apply changes to this folder, subfolders, and files** (Wijzigingen op deze map, onderliggende mappen en bestanden toepassen)
4. Klik op **OK**.

Gecodeerde e-mail versturen en ontvangen

Dankzij Embedded Security kunt u gecodeerde e-mail verzenden en ontvangen, maar de procedures zijn afhankelijk van het e-mailprogramma dat u gebruikt. Raadpleeg voor meer informatie de online Help voor Embedded Security for ProtectTools en de online Help voor uw e-mailprogramma.

Wachtwoord voor de Basic User Key wijzigen

U wijzigt als volgt het wachtwoord voor de Basic User Key:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Geïntegreerde beveiliging** en vervolgens op **Beveiliging**.
3. Klik in het rechterdeelvenster onder **Basic User Key password** (Wachtwoord Basic User Key) op **Wijzigen**.
4. Typ het huidige wachtwoord, en typ en bevestig vervolgens het nieuwe wachtwoord.
5. Klik op **OK**.

Geavanceerde taken

Backup maken en herstellen

De backupvoorziening van Embedded Security maakt een archief met certificeringsinformatie die in geval van nood hersteld kan worden.

Backups maken

U maakt als volgt een backup:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Geïntegreerde beveiliging** en vervolgens op **Backup**.
3. Klik in het rechterdeelvenster op **Backup**. De HP Embedded Security for ProtectTools wizard Backup wordt geopend.
4. Volg de instructies op het scherm.

Certificeringsgegevens herstellen vanuit het backupbestand

U herstelt als volgt gegevens vanuit het backupbestand:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Geïntegreerde beveiliging** en vervolgens op **Backup**.
3. Klik in het rechterdeelvenster op **Herstellen**. De HP Embedded Security for ProtectTools wizard Backup wordt geopend.
4. Volg de instructies op het scherm.

Eigenaarswachtwoord wijzigen

U wijzigt als volgt het eigenaarswachtwoord:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Geïntegreerde beveiliging** en vervolgens op **Geavanceerd**.
3. Klik in het rechterdeelvenster onder **Owner Password** (Eigenaarswachtwoord) op **Wijzigen**.
4. Typ het huidige eigenaarswachtwoord. Typ vervolgens het nieuwe wachtwoord en bevestig dit.
5. Klik op **OK**.

Gebruikerswachtwoord herstellen

Een beheerder kan een gebruiker helpen een vergeten wachtwoord te herstellen. Raadpleeg voor meer informatie de online Help.

Embedded Security in- en uitschakelen

U kunt de voorzieningen van Embedded Security uitschakelen als u zonder de beveiligingsfunctie wilt werken.

De voorzieningen van Embedded Security kunt u op twee verschillende niveaus in- of uitschakelen:

- Tijdelijk uitschakelen: Met deze optie wordt de geïntegreerde beveiliging automatisch weer ingeschakeld wanneer Windows opnieuw wordt opgestart. Deze optie is standaard beschikbaar voor alle gebruikers.
- Blijvend uitschakelen: Met deze optie heeft u het eigenaarswachtwoord nodig om Embedded Security opnieuw in te schakelen. Deze optie is alleen beschikbaar voor beheerders.

Embedded Security blijvend uitschakelen

U schakelt Embedded Security als volgt blijvend uit:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Geïntegreerde beveiliging** en vervolgens op **Geavanceerd**.
3. Klik in het rechterdeelvenster onder **Embedded Security Features** (Voorzieningen Embedded Security) op **Uitschakelen**.
4. Voer uw eigenaarswachtwoord wanneer u daarom wordt gevraagd en klik vervolgens op **OK**.

Embedded Security weer inschakelen na blijvend uitschakelen

U schakelt Embedded Security als volgt in nadat het blijvend uitgeschakeld is:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Geïntegreerde beveiliging** en vervolgens op **Geavanceerd**.
3. Klik in het rechterdeelvenster onder **Embedded Security Features** (Voorzieningen Embedded Security) op **Enable** (Inschakelen).
4. Voer uw eigenaarswachtwoord wanneer u daarom wordt gevraagd en klik vervolgens op **OK**.

Sleutels migreren met de wizard Migreren

Migreren is een taak waarmee het beheren, herstellen en overzetten van sleutels en certificaten wordt uitgevoerd.

Raadpleeg de Help bij Embedded Security voor meer informatie over migratie.

4 Java Card Security for HP ProtectTools

Java Card Security for HP ProtectTools beheert de installatie en configuratie van Java Cards voor computers die zijn uitgerust met een optionele kaartlezer.

Met Java Card Security for HP ProtectTools kunt u het volgende doen:

- De beveiligingsopties voor Java Cards openen.
- Het hulpprogramma Computer Setup (Computerinstellingen) gebruiken om Java Card-verificatie in te schakelen in een opstartomgeving.
- Afzonderlijke Java Cards configureren voor een beheerder en een gebruiker. Hiervoor moet de gebruiker de Java Card plaatsen en een pincode invoeren voordat het besturingssysteem wordt geladen.
- Pincode instellen en wijzigen die wordt gebruikt om gebruikers van de Java Card te verifiëren.

Algemene taken

Op de pagina “Algemeen” kunt u de volgende taken uitvoeren:

- de pincode van een Java Card wijzigen
- de kaartlezer selecteren



OPMERKING: De kaartlezer gebruikt zowel Java Cards als Smart Cards. Deze voorziening is beschikbaar als uw computer is voorzien van meer dan één kaartlezer.

Pincode van een Java Card wijzigen

U wijzigt als volgt de pincode van een Java Card:



OPMERKING: De pincode van de Java Card moet uit 4 tot 8 cijfers bestaan.

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Java Card Security** en vervolgens op **Algemeen**.
3. Plaats een Java Card (met een bestaande pincode) in de kaartlezer.
4. Klik in het rechterdeelvenster op **Wijzigen**.
5. Typ in het dialoogvenster **Pincode wijzigen** de huidige pincode in het vak **Huidige pincode**.
6. Typ de nieuwe pincode in het vak **Nieuwe pincode** en dan nogmaals in het vak **Bevestig de nieuwe pincode**.
7. Klik op **OK**.

Kaartlezer selecteren

Controleer voordat u de Java Card gebruikt of de juiste kaartlezer is geselecteerd in Java Card Security. Als niet de juiste lezer is geselecteerd, zijn sommige voorzieningen mogelijk niet beschikbaar, of worden ze onjuist weergegeven. Daarnaast moeten de stuurprogramma's voor de kaartlezer correct zijn geïnstalleerd, zoals wordt getoond in Windows Apparaatbeheer.

U selecteert als volgt een kaartlezer:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Java Card Security** en vervolgens op **Algemeen**.
3. Plaats de Java Card in de kaartlezer.
4. Klik in het rechterdeelvenster op de juiste lezer onder **Selected Card Reader** (Geselecteerde kaartlezer).

Geavanceerde taken (alleen beheerders)

Op de pagina “Geavanceerd” kunt u de volgende taken uitvoeren:

- een pincode toewijzen aan een Java Card
- een naam toewijzen aan een Java Card
- opstartverificatie instellen
- backup maken en herstellen van Java Cards



OPMERKING: De pagina “Geavanceerd” kan alleen worden weergegeven als u Windows-beheerdersrechten heeft.

Pincode toewijzen aan een Java Card

Voordat een Java Card kan worden gebruikt in Java Card Security, moeten een naam en een pincode aan de Java Card zijn toegewezen.

U wijst als volgt een pincode toe aan een Java Card:



OPMERKING: De pincode van de Java Card moet uit 4 tot 8 cijfers bestaan.

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Java Card Security** en vervolgens op **Geavanceerd**.
3. Plaats een nieuwe Java Card in de kaartlezer.
4. Wanneer het dialoogvenster **Nieuwe kaart** wordt geopend, typt u een nieuwe pincode in het vak **Nieuwe weergavenaam**. Typ een nieuwe pincode in het vak en nogmaals in het vak **Nieuwe pincode bevestigen**.
5. Klik op **OK**.

Naam toewijzen aan een Java Card

Voordat een Java Card kan worden gebruikt voor opstartverificatie, moet een naam aan de Java Card zijn toegewezen.

U wijst als volgt een naam toe aan een Java Card:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Java Card Security** en vervolgens op **Geavanceerd**.
3. Plaats de Java Card in de kaartlezer.



OPMERKING: Als u geen pincode heeft toegewezen aan deze Java Card, wordt het dialoogvenster **Nieuwe kaart** geopend, waar u een nieuwe naam en pincode kunt invoeren.

4. Klik in het rechterdeelvenster onder **Weergavenaam** op **Wijzigen**.
5. Typ een naam voor de Java Card in het vak **Naam**.

6. Typ de huidige pincode voor de Java Card in het vak **Pincode**.
7. Klik op **OK**.

Opstartverificatie instellen

Als opstartverificatie is ingeschakeld, heeft u een Java Card nodig om de computer op te starten.

Voor het instellen van de Java Card-opstartbeveiliging voert u de volgende stappen uit:

1. Schakel ondersteuning voor opstartverificatie met Java Card in BIOS Configuration of in Computer Setup (Computerinstellingen) in. Raadpleeg "[Ondersteuning voor opstartverificatie met Smart Card in- en uitschakelen op pagina 47](#)" voor meer informatie.
2. Schakel opstartverificatie in Java Card-beveiliging in.
3. Java Card voor beheerder maken en inschakelen.

Opstartverificatie met Java Card inschakelen en een beheerders-Java Card maken

U schakelt opstartverificatie met Java Cards als volgt in:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Java Card Security** en vervolgens op **Geavanceerd**.
3. Plaats de Java Card in de kaartlezer.



OPMERKING: Als u geen naam en pincode heeft toegewezen aan deze Java Card, wordt het dialoogvenster **Nieuwe kaart** geopend, waar u een nieuwe naam en pincode kunt invoeren.

4. Schakel in het rechterdeelvenster onder **Verificatie bij opstarten** het selectievakje **Enable** (Inschakelen) in.
5. Typ uw instelwachtwoord voor Computer Setup (Computerinstellingen) in het dialoogvenster **Wachtwoord voor Computer Setup**. Klik vervolgens op **OK**.
6. Als u DriveLock niet heeft ingeschakeld, voert u de pincode van de Java Card in. Klik vervolgens op **OK**.

– of –

Als u DriveLock wel heeft ingeschakeld, doet u het volgende:

- a. Klik op **Maak identiteit van Java Card uniek**.

– of –

Klik op **Maak de identiteit van de Java Card gelijk aan het DriveLock wachtwoord**.



OPMERKING: Als DriveLock is ingeschakeld op uw computer, kunt u het DriveLock gebruikerswachtwoord instellen als de identiteit van de Java Card, waardoor u met de Java Card direct zowel DriveLock als de Java Card kunt valideren wanneer u de computer opstart.

- b. Indien van toepassing, typt u uw DriveLock gebruikerswachtwoord in het vakje **DriveLock-wachtwoord** en dan nogmaals in het vakje **Wachtwoord bevestigen**.

- c. Voer de pincode van de Java Card in.
 - d. Klik op **OK**.
7. Als u wordt gevraagd of u een herstelbestand wilt aanmaken, klikt u op **Annuleren** om op een later tijdstip een herstelbestand te maken. Als u nu een herstelbestand wilt maken, klikt u op **OK** en volgt u de aanwijzingen op het scherm in de wizard Backup van HP ProtectTools.



OPMERKING: Raadpleeg "[HP ProtectTools Backup en herstellen op pagina 9](#)" voor meer informatie.

Gebruikers-Java Card maken



OPMERKING: Opstartverificatie en een beheerders-Java Card moeten zijn ingesteld voordat u een gebruikers-Java Card kunt maken.

U maakt als volgt een gebruikers-Java Card:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Java Card Security** en vervolgens op **Geavanceerd**.
3. Plaats een Java Card die als gebruikerskaart zal worden gebruikt.
4. Klik in het rechterdeelvenster onder **Verificatie bij opstarten** naast **Identiteit van gebruikerskaart** op **Maken**.
5. Voer een pincode in voor de Java Card en klik op **OK**.

Opstartverificatie met Java Card uitschakelen

Als u opstartverificatie met Java Card uitschakelt, heeft u geen Java Card meer nodig om toegang te krijgen tot de computer.

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Java Card Security** en vervolgens op **Geavanceerd**.
3. Plaats de beheerder-Java Card in de kaartlezer.
4. Schakel in het rechterdeelvenster onder **Verificatie bij opstarten** het selectievakje **Enable** (Inschakelen) uit.
5. Voer een pincode in voor de gebruikers-Java Card en klik op **OK**.

5 BIOS Configuration for HP ProtectTools

BIOS Configuration for HP ProtectTools biedt toegang tot beveiligings- en configuratie-instellingen van Computer Setup (Computerinstellingen). Hierdoor hebben Windows-gebruikers toegang tot de systeembeveiligingsfuncties die met Computer Setup (Computerinstellingen) worden beheerd.

Met BIOS Configuration for HP ProtectTools kunt u het volgende doen:

- Opstart- en beheerderswachtwoorden beheren.
- Andere opstartverificatiefuncties instellen, zoals aanmelden bij de geïntegreerde beveiliging.
- Hardwarefuncties in- en uitschakelen, zoals bijvoorbeeld opstarten vanaf een cd-rom of andere hardwarepoorten.
- Opstartopties instellen, waaronder MultiBoot en een gewijzigde opstartvolgorde.



OPMERKING: Veel van de voorzieningen in BIOS Configuration for HP ProtectTools zijn ook beschikbaar in Computer Setup (Computerinstellingen).

Algemene taken

Met BIOS Configuration kunt u verschillende computerinstellingen beheren die anders alleen toegankelijk zouden zijn door bij het opstarten op **f10** te drukken en Computer Setup (Computerinstellingen) te openen.

Opstartopties beheren

U kunt BIOS Configuration gebruiken voor het beheren van verschillende instellingen taken die worden uitgevoerd wanneer u de computer (opnieuw) opstart.

U beheert opstartopties als volgt:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **BIOS-configuratie**.
3. Voer uw beheerderswachtwoord van Computer Setup (Computerinstellingen) in als om het BIOS-beheerderswachtwoord wordt gevraagd en klik op **OK**.



OPMERKING: Er wordt alleen om het BIOS-beheerderswachtwoord gevraagd als u het wachtwoord voor Computer Setup (Computerinstellingen) al heeft ingesteld. Raadpleeg "[Instelwachtwoord instellen op pagina 49](#)" voor meer informatie over het instellen van het wachtwoord voor Computer Setup (Computerinstellingen).

4. Klik in het linkerdeelvenster op **Systeemconfiguratie**.
5. Selecteer in het rechterdeelvenster de vertragingen (in seconden) voor **f9**, **f10**, **f12** en voor **Weergave Expres Boot-menu (in seconden)**.
6. **MultiBoot** in- of uitschakelen.
7. Als u MultiBoot heeft ingeschakeld, selecteert u de opstartvolgorde door een opstartapparaat te selecteren en vervolgens op de pijl-omhoog of de pijl-omlaag te klikken om de volgorde in de lijst te wijzigen.
8. Klik in het venster HP ProtectTools op **Apply** (Toepassen) en vervolgens op **OK**.

Systeemconfiguratieopties in- en uitschakelen



OPMERKING: Sommige van de hieronder genoemde opties worden mogelijk niet ondersteund door uw computer.

U schakelt apparaat- of beveiligingsopties als volgt in of uit:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **BIOS-configuratie**.
3. Voer uw beheerderswachtwoord van Computer Setup (Computerinstellingen) in als om het BIOS-beheerderswachtwoord wordt gevraagd en klik op **OK**.

4. Klik in het linkerdeelvenster op **Systeemconfiguratie** en schakel vervolgens een systeemconfiguratieoptie in of uit, of configureer in het rechterdeelvenster een van de opties voor de volgende systeemonderdelen:

- Poortopties
 - Seriële poort
 - Infraroodpoort
 - Parallele poort
 - SD Slot (SD-slot)
 - USB-poort
 - 1394-poort
 - CardBus-slot
 - ExpressCard-slot
- Opstartopties
 - Vertraging voor f9, f10 en f12 (in seconden)
 - MultiBoot
 - Weergave Express Boot-menu (in seconden)
 - Opstarten vanaf cd-rom-drive
 - Opstarten vanaf diskettedrive
 - Opstarten vanaf interne netwerkadapter
 - Opstarten vanaf interne netwerkadapter (PXE of RPL)
 - Opstartvolgorde
- Apparaatconfiguraties
 - NumLock at Boot (NumLock bij opstarten)
 - Swapping fn/Ctrl Keys (Fn/Ctrl-toetsen omwisselen)
 - Meerdere aanwijsapparaten
 - Ondersteuning voor Legacy USB
 - Parallele-poortstand (standaard, bidirectioneel, EPP of ECP)
 - Preventie van uitvoering van gegevens
 - Native SATA-modus
 - Processor met dubbele kern
 - Automatische ondersteuning voor Intel® SpeedStep-functionaliteit
 - Ventilator altijd aan bij netvoeding

- BIOS DMA-gegevensoverdrachten
 - Intel or AMD PSAE Execution Disable (Intel- of AMD PSAE-uitvoering uitschakelen)
 - Ingebouwde apparaatopties
 - Geïntegreerde radio van WLAN-apparaat
 - Geïntegreerde radio van WWAN-apparaat
 - Geïntegreerde radio van Bluetooth®-apparaat
 - Schakelen tussen LAN/WLAN
 - Inschakelen via Wake On Lan
5. Klik op **Apply** (Toepassen) en vervolgens op **OK** in het venster van HP ProtectTools om uw wijzigingen op te slaan en het programma af te sluiten.

Geavanceerde taken

Instellingen Van aanvullende module voor HP ProtectTools beheren

Enkele van de voorzieningen van HP ProtectTools Security Manager kunnen worden beheerd in BIOS Configuration.

Ondersteuning voor opstartverificatie met Smart Card in- en uitschakelen

Door deze optie in te schakelen kunt u een Smart Card voor gebruikersverificatie gebruiken wanneer u de computer aanzet.



OPMERKING: Als u de opstartverificatievoorziening volledig wilt inschakelen, is het noodzakelijk om ook een Smart Card te configureren met de module Java Card Security for HP ProtectTools.

U schakelt opstartverificatie met Smart Cards als volgt in:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **BIOS-configuratie**.
3. Voer uw beheerderswachtwoord van Computer Setup (Computerinstellingen) in als om het BIOS-beheerderswachtwoord wordt gevraagd en klik op **OK**.
4. Klik in het linkerdeelvenster op **Beveiliging**.
5. Klik op **Inschakelen** onder **Smart Card-beveiliging**.



OPMERKING: Als u opstartverificatie met Smart Card wilt uitschakelen, klikt u op **Disable** (Uitschakelen).

6. Klik in het venster HP ProtectTools op **Apply** (Toepassen) en vervolgens op **OK**.

Opstartverificatie via geïntegreerde beveiligingschip in- en uitschakelen

Door deze optie in te schakelen kan de geïntegreerde TPM-beveiligingschip (indien beschikbaar) worden gebruikt voor gebruikersverificatie wanneer u de computer aanzet.



OPMERKING: Als u de functie opstartverificatie volledig wilt inschakelen, is het noodzakelijk om ook de geïntegreerde TPM-beveiligingschip te configureren met de module Embedded Security for HP ProtectTools.

U schakelt ondersteuning voor opstartverificatie met geïntegreerde beveiliging als volgt in:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **BIOS-configuratie**.
3. Voer uw beheerderswachtwoord van Computer Setup (Computerinstellingen) in als om het BIOS-beheerderswachtwoord wordt gevraagd en klik op **OK**.
4. Klik in het linkerdeelvenster op **Beveiliging**.
5. Klik op **Verificatie bij opstarten activeren** onder **Geïntegreerde beveiliging**.



OPMERKING: Als u opstartverificatie met geïntegreerde beveiliging wilt uitschakelen, klikt u op **Disable** (Uitschakelen).

6. Klik in het venster HP ProtectTools op **Apply** (Toepassen) en vervolgens op **OK**.

Beveiliging van vaste schijf met Automatic DriveLock in- en uitschakelen

Als deze optie is ingeschakeld worden de DriveLock wachtwoorden automatisch gegenereerd, ingesteld in de schijf eenheid en beschermd door de geïntegreerde TPM-beveiligingschip.



OPMERKING: De automatisch gegenereerde wachtwoorden worden pas in de schijf eenheid ingesteld als de computer opnieuw wordt opgestart en u het juiste wachtwoord voor geïntegreerde TPM-beveiliging heeft ingevoerd.

De optie om Automatic DriveLock in te schakelen is alleen beschikbaar als een TPM-beveiligingschip in de computer is geïnstalleerd en geïnitieerd, en geen DriveLock wachtwoorden zijn ingeschakeld. Raadpleeg "[Embedded Security for ProtectTools op pagina 30](#)" en "[Geïntegreerde beveiligingschip initialiseren op pagina 30](#)" voor instructies voor het inschakelen en initialiseren van de TPM-beveiligingschip.



OPMERKING: Als u al handmatig DriveLock wachtwoorden op de computer heeft ingesteld, schakelt u deze eerst uit voordat u bescherming door Automatic DriveLock kunt instellen.

U schakelt bescherming met Automatic DriveLock als volgt in of uit:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **BIOS-configuratie**.
3. Voer uw beheerderswachtwoord van Computer Setup (Computerinstellingen) in als om het BIOS-beheerderswachtwoord wordt gevraagd en klik op **OK**.
4. Klik in het linkerdeelvenster op **Beveiliging**.
5. Klik onder **Embedded Security** naast **Automatic DriveLock Support** (Ondersteuning voor Automatic DriveLock) op **Enable** (Inschakelen).



OPMERKING: Als u bescherming met Automatic DriveLock voor geïntegreerde beveiliging wilt uitschakelen, klikt u op **Disable** (Uitschakelen).

6. Klik in het venster HP ProtectTools op **Apply** (Toepassen) en vervolgens op **OK**.

Wachtwoorden van Computer Setup (Computerinstellingen) beheren

U kunt BIOS Configuration gebruiken voor het instellen en wijzigen van opstart- en instelwachtwoorden in Computer Setup (Computerinstellingen) en voor het beheren van verschillende wachtwoordinstellingen.



VOORZICHTIG: De wachtwoorden die u instelt met de pagina "Passwords" (Wachtwoorden) in BIOS Configuration worden direct opgeslagen wanneer u op **Apply** (Toepassen) of **OK** klikt in het venster van HP ProtectTools. Onthoud het ingestelde wachtwoord goed: u kunt een wachtwoordinstelling niet ongedaan maken zonder eerst het oude wachtwoord te hebben ingevoerd.

Met het opstartwachtwoord voorkomt u dat de notebookcomputer wordt gebruikt door onbevoegden.



OPMERKING: Nadat u een opstartwachtwoord heeft ingesteld, wordt de knop Set (Instellen) op de pagina “Passwords” (Wachtwoorden) vervangen door een knop Change (Wijzigen).

Met het wachtwoord van Computer Setup (Computerinstellingen) beveiligt u de configuratie-instellingen en de systeemidentificatiegegevens in Computer Setup. Wanneer dit wachtwoord is ingesteld, gebruikt u het om toegang te krijgen tot Computer Setup (Computerinstellingen). Als u een instelwachtwoord heeft ingesteld, wordt u om het wachtwoord gevraagd voordat u het gedeelte BIOS Configuration for HP ProtectTools kunt openen.



OPMERKING: Nadat u een instelwachtwoord heeft ingesteld, wordt de knop Set (Instellen) op de pagina “Passwords” (Wachtwoorden) vervangen door een knop Change (Wijzigen).

Opstartwachtwoord instellen

U stelt het opstartwachtwoord als volgt in:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **BIOS-configuratie** en vervolgens op **Beveiliging**.
3. Klik in het rechterdeelvenster naast **Opstartwachtwoord** op **Instellen**.
4. Typ en bevestig het wachtwoord in de vakken **Wachtwoord opgeven** en **Wachtwoord bevestigen**.
5. Klik op **OK** in het dialoogvenster Passwords (Wachtwoorden).
6. Klik in het venster HP ProtectTools op **Apply** (Toepassen) en vervolgens op **OK**.

Opstartwachtwoord wijzigen

U wijzigt het opstartwachtwoord als volgt:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **BIOS-configuratie** en vervolgens op **Beveiliging**.
3. Klik in het rechterdeelvenster naast **Opstartwachtwoord** op **Wijzigen**.
4. Typ het huidige hoofdwachtwoord in het vak **Oud wachtwoord**.
5. Typ en bevestig het nieuwe wachtwoord in het vak **Nieuw wachtwoord**.
6. Klik op **OK** in het dialoogvenster Passwords (Wachtwoorden).
7. Klik in het venster HP ProtectTools op **Apply** (Toepassen) en vervolgens op **OK**.

Instelwachtwoord instellen

U stelt het wachtwoord voor Computer Setup (Computerinstellingen) als volgt in:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **BIOS-configuratie** en vervolgens op **Beveiliging**.
3. Klik in het rechterdeelvenster naast **Instelwachtwoord** op **Instellen**.

4. Typ en bevestig het wachtwoord in de vakken **Wachtwoord opgeven** en **Wachtwoord bevestigen**.
5. Klik op **OK** in het dialoogvenster Passwords (Wachtwoorden).
6. Klik in het venster HP ProtectTools op **Apply** (Toepassen) en vervolgens op **OK**.

Instelwachtwoord wijzigen

U wijzigt het wachtwoord voor Computer Setup (Computerinstellingen) als volgt:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **BIOS-configuratie** en vervolgens op **Beveiliging**.
3. Klik in het rechterdeelvenster naast **Instelwachtwoord** op **Wijzigen**.
4. Typ het huidige hoofdwachtwoord in het vak **Oud wachtwoord**.
5. Typ en bevestig het nieuwe wachtwoord in de vakken **Nieuw wachtwoord** en **Nieuw wachtwoord bevestigen**.
6. Klik op **OK** in het dialoogvenster Passwords (Wachtwoorden).
7. Klik in het venster HP ProtectTools op **Apply** (Toepassen) en vervolgens op **OK**.

Wachtwoordopties instellen

U kunt met BIOS Configuration for HP ProtectTools wachtwoordopties instellen om uw systeem beter te beveiligen.

Strengere beveiliging in- en uitschakelen



VOORZICHTIG: Noteer het door u ingestelde instellingenwachtwoord, opstartwachtwoord of de door u ingestelde Smart Card-pincode en bewaar dit op een veilige plaats uit de buurt van uw computer om te voorkomen dat deze permanent onbruikbaar wordt. Zonder deze wachtwoorden of pincode kan de computer niet worden ontgrendeld.

Met strenge beveiliging krijgt u nog betere bescherming dankzij de opstart- en beheerderswachtwoorden en andere vormen van opstartverificatie.

U schakelt strenge beveiliging als volgt in of uit:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **BIOS-configuratie** en vervolgens op **Beveiliging**.
3. Schakel in het rechterdeelvenster **Strengere beveiliging** onder **Wachtwoordopties** in of uit.



OPMERKING: Als u strenge beveiliging wilt uitschakelen, schakelt u het selectievakje **Enable Stringent Security** (Strenge beveiliging inschakelen) uit.

4. Klik in het venster HP ProtectTools op **Apply** (Toepassen) en vervolgens op **OK**.

Opstartverificatie bij het opnieuw opstarten van Windows in- en uitschakelen

Met deze optie kunt u de beveiliging verbeteren door te eisen dat gebruikers een opstart-, TPM- of Smart Card-wachtwoord invoeren wanneer Windows opnieuw wordt opgestart.

U schakelt opstartverificatie bij het opnieuw opstarten van Windows als volgt in of uit:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **BIOS-configuratie** en vervolgens op **Beveiliging**.
3. Schakel in het rechterdeelvenster **Wachtwoord vereist bij herstart** onder **Wachtwoordopties** in of uit.
4. Klik in het venster HP ProtectTools op **Apply** (Toepassen) en vervolgens op **OK**.

6 Device Access Manager for HP ProtectTools

Dit beveiligingshulpmiddel is alleen beschikbaar voor beheerders. Device Access Manager for HP ProtectTools is voorzien van de volgende beveiligingsfuncties die bescherming bieden tegen ongeoorloofde toegang tot apparaten die zijn aangesloten op uw computersysteem:

- Voor elke gebruiker wordt een apparaatprofiel gemaakt waarmee toegang tot apparatuur wordt bepaald
- Toegang tot een apparaat kan worden toegestaan of geweigerd op basis van lidmaatschap van een groep

Achtergrondservice starten

Zorg ervoor dat de achtergrondservice HP ProtectTools Device Locking/Auditing wordt uitgevoerd als u apparaatprofielen wilt toepassen. Wanneer u voor de eerste keer apparaatprofielen toepast, opent de HP ProtectTools Security Manager een dialoogvenster waarin u wordt gevraagd of u de achtergrondservice wilt starten. Klik op **Yes** (Ja) om de achtergrondservice te starten en zo in te stellen dat deze iedere keer dat het systeem opstart automatisch wordt opgestart.

Eenvoudige configuratie

Met de voorziening Eenvoudige configuratie kunt u de toegang tot volgende apparaatklassen weigeren:

- USB-apparaten voor alle niet-beheerders
- Alle verwijderbare media (floppydisks, penschijven, etc.) voor alle niet-beheerders
- Alle dvd-/cd-rom-drives voor alle niet-beheerders
- Alle seriële en parallelle poorten voor alle niet-beheerders

Ga als volgt te werk om in te stellen dat alle niet-beheerders de toegang tot een apparaatklasse wordt geweigerd:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Device Access Manager** en vervolgens op **Eenvoudige configuratie**.
3. Selecteer in het rechterdeelvenster het selectievakje van een apparaat om het apparaat toegang te weigeren.
4. Klik op **Apply** (Toepassen).



OPMERKING: Als de achtergrondservice niet wordt uitgevoerd, probeert deze nu op te starten. Klik op **Yes** (Ja) om dit toe te staan.

5. Klik op **OK**.

Configuratie van apparaatklassen (geavanceerd)

Meerdere selecties zijn beschikbaar, waarmee u verschillende gebruikers of groepen toegang tot bepaalde apparaattypen kunt verlenen of weigeren.

Gebruiker of groep toevoegen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Device Access Manager** en vervolgens op **Apparaatklasseconfiguratie**.
3. Klik in de apparaatlijst op de apparaatklasse die u wilt configureren.
4. Klik op **Toevoegen**. Het dialoogvenster **Select Users or Groups** (Gebruikers of groepen selecteren) wordt geopend.
5. Selecteer **Geavanceerd > Find Now** (Nu zoeken) om gebruikers of groepen te zoeken die u kunt toevoegen.
6. Klik op een gebruiker of een groep die u aan de lijst van beschikbare gebruikers en groepen wilt toevoegen en klik vervolgens op **OK**.
7. Klik op **OK**.

Gebruiker of groep verwijderen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Device Access Manager** en vervolgens op **Apparaatklasseconfiguratie**.
3. Klik in de apparaatlijst op de apparaatklasse die u wilt configureren.
4. Klik op de gebruiker of groep die u wilt verwijderen en klik op **Remove** (Verwijderen).
5. Klik op **Apply** (Toepassen) en vervolgens op **OK**.

Gebruiker of groep toegang weigeren

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Device Access Manager** en vervolgens op **Apparaatklasseconfiguratie**.
3. Klik in de apparaatlijst op de apparaatklasse die u wilt configureren.
4. Klik onder **User/Groups** (Gebruiker/groepen) op de gebruiker of groep toe die u toegang wilt weigeren.
5. Klik op **Weigeren** naast de gebruiker of groep toe die u toegang wilt weigeren.
6. Klik op **Apply** (Toepassen) en vervolgens op **OK**.

Toegang tot een apparaatklasse verlenen aan één gebruiker van een groep

U kunt één gebruiker toegang verlenen tot een apparaatklasse terwijl u anderen in die gebruikersgroep toegang weigert.

U verleent als volgt toegang aan één gebruiker, maar niet aan de hele groep:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Device Access Manager** en vervolgens op **Apparaatklasseconfiguratie**.
3. Klik in de apparaatlijst op de apparaatklasse die u wilt configureren.
4. Voeg onder **User/Groups** (Gebruiker/groepen) de groep toe die u toegang wilt weigeren.
5. Klik op **Weigeren** naast de groep toe die u toegang wilt weigeren.
6. Navigeer naar de map onder die van de vereiste klasse en voeg de specifieke gebruiker toe. Klik op **Toestaan** om deze gebruiker toegang te verlenen.
7. Klik op **Apply** (Toepassen) en vervolgens op **OK**.

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

U kunt één gebruiker toegang verlenen tot een specifiek apparaat terwijl u anderen in die gebruikersgroep toegang weigert tot alle apparatuur in die klasse.

U verleent als volgt toegang tot een specifiek apparaat aan één gebruiker, maar niet aan de hele groep:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Device Access Manager** en vervolgens op **Apparaatklasseconfiguratie**.
3. Klik in de apparaatlijst op de apparaatklasse die u wilt configureren en navigeer vervolgens naar de map onder deze klasse.
4. Voeg onder **User/Groups** (Gebruiker/groepen) de groep toe die u toegang wilt weigeren.
5. Klik op **Weigeren** naast de groep toe die u toegang wilt weigeren.
6. Navigeer naar het specifieke apparaat waartoe u de gebruiker in de apparaatlijst toegang wilt verlenen.
7. Klik op **Toevoegen**. Het dialoogvenster **Select Users or Groups** (Gebruikers of groepen selecteren) wordt geopend.
8. Selecteer **Geavanceerd > Find Now** (Nu zoeken) om gebruikers of groepen te zoeken die u kunt toevoegen.
9. Klik op een gebruiker die u toegang wilt verlenen en klik vervolgens op **OK**.
10. Klik op **Toestaan** om deze gebruiker toegang te verlenen.
11. Klik op **Apply** (Toepassen) en vervolgens op **OK**.

7 Drive Encryption for HP ProtectTools



VOORZICHTIG: Als u de module Drive Encryption wilt verwijderen, decodeert u eerst alle gecodeerde schijven. Als u dit niet doet, heeft u geen toegang meer tot de gegevens op gecodeerde schijven, tenzij u zich heeft aangemeld bij de Drive Encryption herstelservice (raadpleeg "[Herstel op pagina 63](#)"). Als u de module Drive Encryption opnieuw installeert, heeft u nog altijd geen toegang tot de gecodeerde schijven.

Coderingsbeheer

Schijf coderen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Drive Encryption** en vervolgens op **Encryption Management** (Coderingsbeheer).
3. Klik in het rechterdeelvenster op **Activate** (Activeren). De wizard Drive Encryption for HP ProtectTools wordt geopend.
4. Volg de instructies op het scherm om de codering te activeren.



OPMERKING: Geef een diskette, flash-opslagapparaat of een ander opslagmedium met USB-aansluiting op waarop u de herstel informatie wilt opslaan.

Codering wijzigen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Drive Encryption** en vervolgens op **Encryption Management** (Coderingsbeheer).
3. Klik in het rechterdeelvenster op **Change encryption** (Codering wijzigen). Selecteer de schijven die u wilt coderen in het dialoogvenster **Change Encryption** (Codering wijzigen) en klik vervolgens op **OK**.
4. Klik nogmaals op **OK** om te beginnen met coderen.

Schijf decoderen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Drive Encryption** en vervolgens op **Encryption Management** (Coderingsbeheer).
3. Klik in het rechterdeelvenster op **Deactivate** (Deactiveren).

Gebruikersbeheer

Gebruiker toevoegen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Drive Encryption** en vervolgens op **User Management** (Gebruikersbeheer).
3. Klik in het rechterdeelvenster op **Add** (Toevoegen). Klik op een gebruikersnaam in het vak **User name** (Gebruikersnaam), of typ een gebruikersnaam in het vak **Username** (Gebruikersnaam). Klik op **Next** (Volgende).
4. Voer het Windows-wachtwoord voor de geselecteerde gebruiker in en klik op **Next** (Volgende).
5. Selecteer een verificatiemethode voor de nieuwe gebruiker en klik op **Next** (Volgende).

Gebruiker verwijderen

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Drive Encryption** en vervolgens op **User Management** (Gebruikersbeheer).
3. Klik in het rechterdeelvenster op de gebruikersnaam die u wilt verwijderen in de lijst **User name** (Gebruikersnaam). Klik op **Verwijderen**.
4. Klik op **Yes** (Ja) om te bevestigen dat u de geselecteerde gebruiker wilt verwijderen.

Token wijzigen

U wijzigt als volgt de verificatiemethode voor een gebruiker:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Drive Encryption** en vervolgens op **User Management** (Gebruikersbeheer).
3. Selecteer in het rechterdeelvenster de gebruikersnaam in de lijst **User name** (Gebruikersnaam) en klik vervolgens op **Change Token** (Token wijzigen).
4. Voer het Windows-wachtwoord van de gebruiker in en klik op **Next** (Volgende).
5. Selecteer een nieuwe verificatiemethode en klik op **Next** (Volgende).
6. Als u Java Card heeft geselecteerd als de verificatiemethode, voert u het wachtwoord van de Java Card in wanneer u daarom wordt gevraagd en klikt u vervolgens op **OK**.

Wachtwoord instellen

U kunt als volgt voor een gebruiker een wachtwoord instellen of de verificatiemethode wijzigen:

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Drive Encryption** en vervolgens op **User Management** (Gebruikersbeheer).
3. Selecteer in het rechterdeelvenster de gebruikersnaam in de lijst **User name** (Gebruikersnaam) en klik vervolgens op **Set Password** (Wachtwoord instellen).

4. Voer het Windows-wachtwoord van de gebruiker in en klik op **Next** (Volgende).
5. Selecteer de nieuwe verificatiemethode en klik op **Next** (Volgende).
6. Als u Java Card heeft geselecteerd als de verificatiemethode, voert u het wachtwoord van de Java Card in wanneer u daarom wordt gevraagd en klikt u vervolgens op **OK**.

Herstel

Neem hierbij de volgende twee veiligheidsmaatregelen in acht:

- Als u uw wachtwoord vergeet, heeft u geen toegang meer tot uw gecodeerde schijven. U kunt zich echter aanmelden bij de Drive Encryption herstelservice, zodat u toegang heeft tot uw computer als u uw wachtwoord mocht vergeten.
- U kunt een backup maken van uw Drive Encryption sleutels op een diskette, flash-opslagapparaat of een ander opslagmedium met USB-aansluiting.

Aanmelden voor Drive Encryption herstelservice

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Drive Encryption** en vervolgens op **Recovery** (Herstellen).
3. Klik in het rechterdeelvenster op **Click here to register** (Klik hier om u aan te melden). Voer de gevraagde gegevens in om de backupprocedure voor beveiliging te voltooien.

Backup maken van uw Drive Encryption sleutels

1. Selecteer **Start > Alle programma's > HP ProtectTools Security Manager**.
2. Klik in het linkerdeelvenster op **Drive Encryption** en vervolgens op **Recovery** (Herstellen).
3. Klik in het rechterdeelvenster op **Click here to backup your keys** (Klik hier om een backup van uw sleutels te maken).
4. Geef een diskette, flash-opslagapparaat of een ander opslagmedium met USB-aansluiting op waarop u de herstel informatie wilt opslaan en klik vervolgens op **Next** (Volgende). De wizard Drive Encryption for HP ProtectTools wordt geopend.
5. Volg de instructies op het scherm om een backup te maken van de Drive Encryption sleutels.



OPMERKING: Geef een diskette, flash-opslagapparaat of een ander opslagmedium met USB-aansluiting op waarop u de herstel informatie wilt opslaan.

8 Problemen oplossen

Credential Manager for HP ProtectTools

Korte beschrijving	Gegevens	Oplossing
Gebruikers kunnen via de optie Credential Manager Network Accounts selecteren bij welke domeinaccount zij zich willen aanmelden. Wanneer verificatie door middel van een TPM-beveiligingschip wordt gebruikt, is deze optie niet beschikbaar. Alle andere verificatiemethoden werken naar behoren.	Bij gebruik van TPM-verificatie is de gebruiker alleen aangemeld bij de lokale computer.	Wanneer gebruikgemaakt wordt van de hulpmiddelen van Credential Manager Single Sign On, kan een gebruiker andere accounts verifiëren.
De referentie voor het USB-token is niet beschikbaar bij het aanmelden wanneer gebruikgemaakt wordt van Windows XP Service Pack 1.	Nadat u de USB-tokensoftware heeft geïnstalleerd, de referentie voor het USB-token heeft geregistreerd en Credential Manager heeft ingesteld als primaire aanmelding, wordt het USB-token niet weergegeven bij het aanmelden via Credential Manager/GINA. Nadat u zich opnieuw bij Windows heeft aangemeld, zich heeft afgemeld en weer aangemeld bij Credential Manager en het token heeft geselecteerd als de primaire aanmelding, functioneert de aanmeldprocedure met het token normaal.	Update Windows naar Service Pack 2 via Windows Update. Als u met Service Pack 1 wilt blijven werken, meldt u zich opnieuw aan bij Windows met een andere referentie (Windows-wachtwoord), zodat u zich kunt afmelden en weer aanmelden bij Credential Manager.
Sommige applicatiewebpagina's veroorzaken fouten waardoor gebruikers taken niet kunnen uitvoeren of voltooiën.	Sommige webapplicaties functioneren dan niet meer en geven foutmeldingen doordat zij worden geblokkeerd door het functionaliteitenpatroon van Single Sign On. In Internet Explorer wordt bijvoorbeeld ! weergegeven in een gele driehoek om aan te geven dat een fout is opgetreden.	Credential Manager Single Sign On ondersteunt niet alle webinterfaces van software. Schakel ondersteuning voor Single Sign On voor de webpagina uit door ondersteuning voor Single Sign On uit te schakelen. Raadpleeg voor meer informatie de volledige documentatie over Single Sign On, die beschikbaar is in de online Help van Credential Manager. Als u een specifieke Single Sign On niet kunt uitschakelen voor een bepaalde applicatie, neemt u telefonisch contact op met de technische ondersteuning van HP en vraagt u uw contactpersoon bij de HP klantenservice om ondersteuning van het derde niveau.
De optie Browse for Virtual Token (Naar virtueel token bladeren) wordt niet weergegeven gedurende het aanmeldproces.	De gebruiker kan de locatie van een geregistreerd virtueel token in Credential Manager niet verplaatsen, omdat de bladeroptie is verwijderd om beveiligingsrisico's te verkleinen.	De bladeroptie is verwijderd, omdat niet-gebruikers bestanden konden verwijderen, bestanden een nieuwe naam konden geven en Windows konden overnemen.
Domeinbeheerders kunnen Windows-wachtwoorden niet wijzigen. Zelfs niet als ze daartoe geautoriseerd zijn.	Dit gebeurt nadat een domeinbeheerder zich aanmeldt bij een domein en de identiteit van het domein bij Credential Manager registreert met een account met beheerdersrechten voor het domein en de lokale computer. Wanneer de domeinbeheerder het Windows-	Credential Manager kan het wachtwoord van een domeingebruiker niet wijzigen via Change Windows password (Windows-wachtwoord wijzigen). Credential Manager kan alleen de accountwachtwoorden voor lokale computers wijzigen. De domeingebruiker kan zijn of haar wachtwoord wijzigen via Windows security > Change password

Korte beschrijving	Gegevens	Oplossing
	wachtwoord probeert te wijzigen vanuit Credential Manager, wordt een foutbericht weergegeven voor de aanmelding: User account restriction (Beperking gebruikersaccount).	(Windows-beveiliging > Wachtwoord wijzigen), maar aangezien de domeingebruiker geen fysieke account heeft op de lokale computer, kan Credential Manager alleen het wachtwoord wijzigen waarmee de gebruiker zich aanmeldt.
Credential Manager heeft compatibiliteitsproblemen met de Corel WordPerfect 12 wachtwoord-GINA.	Als de gebruiker zich aanmeldt bij Credential Manager, een document maakt in WordPerfect en het opslaat met wachtwoordbeveiliging, kan Credential Manager de wachtwoord-GINA niet handmatig of automatisch detecteren of herkennen.	HP onderzoekt mogelijkheden waarop dit probleem bij toekomstige productverbeteringen opgelost kan worden.
Credential Manager herkent de knop Connect (Verbinden) op het scherm niet.	Als de Single Sign On referenties voor Remote Desktop Connection (RDP) zijn ingesteld op Connect (Verbinden) wanneer Single Sign On opnieuw wordt gestart, wordt altijd Save As (Opslaan als) ingevoerd in plaats van Connect (Verbinden).	HP onderzoekt mogelijkheden waarop dit probleem bij toekomstige productverbeteringen opgelost kan worden.
Gebruikers kunnen alle Credential Manager referenties verliezen die worden beschermd door de TPM.	Als de TPM-module wordt verwijderd of beschadigd, verliezen gebruikers alle referenties die worden beschermd door de TPM.	Dit is zo ontworpen. De TPM-module is ontworpen ter bescherming van de Credential Manager referenties. HP adviseert gebruikers een backup te maken van hun identiteit vanuit Credential Manager, voordat zij de TPM-module verwijderen.
De gebruiker kan zich niet aanmelden bij Credential Manager na een overgang van de slaapstand naar de hibernationstand in Windows XP (alleen Service Pack 1).	Nadat het systeem is overgeschakeld van de slaapstand naar de hibernationstand, kunnen de beheerder en gebruikers zich niet meer aanmelden bij Credential Manager en wordt het aanmeldscherm van Windows continu weergegeven, ongeacht welke aanmeldreferentie (wachtwoord, vingerafdruk of Java Card) wordt geselecteerd.	Update Windows naar Service Pack 2 via Windows Update. Raadpleeg artikel nummer 813301 in de Microsoft knowledge base op http://www.microsoft.com voor meer informatie over de oorzaak van dit probleem. Als de gebruiker zich wil aanmelden, selecteert hij of zij Credential Manager en meldt hij of zij zich aan. Nadat de gebruiker zich heeft aangemeld bij Credential Manager, wordt hij of zij gevraagd zich aan te melden bij Windows (mogelijk moet de gebruiker de Windows-aanmeldoptie selecteren) om het aanmeldproces te voltooien. Als de gebruiker zich eerst bij Windows aanmeldt, zal hij of zij zich handmatig moeten aanmelden bij Credential Manager.
Als Embedded Security wordt hersteld werkt Credential Manager niet.	Credential Manager registreert geen referenties nadat het ROM is hersteld naar de fabrieksinstellingen.	Credential Manager maakt geen verbinding met de TPM als het ROM is hersteld naar de fabrieksinstellingen nadat Credential Manager is geïnstalleerd. U kunt de geïntegreerde TPM-beveiligingschip inschakelen via het hulpprogramma f10 Computer Setup (Computerinstellingen), BIOS Configuration of

Korte beschrijving	Gegevens	Oplossing
		HP Client Manager. Volg de stappen hieronder om de geïntegreerde TPM-beveiligingschip in te schakelen. 1. Open Computer Setup (Computerinstellingen) door de computer aan te zetten of opnieuw te starten en op f10 te drukken wanneer het bericht f10 = ROM Based Setup linksonder op het scherm verschijnt. 2. Gebruik de pijltoetsen om Beveiliging > Instelwachtwoord te selecteren. Stel een wachtwoord in. 3. Selecteer Embedded Security Device (Geïntegreerd beveiligingsapparaat). 4. Gebruik de pijltoetsen om Embedded Security Device—Disable (Geïntegreerd beveiligingsapparaat – uitschakelen) te selecteren. Gebruik de pijltoetsen om deze instelling te wijzigen naar Embedded Security Device—Disable (Geïntegreerd beveiligingsapparaat – inschakelen). 5. Selecteer Enable > Save changes and exit (Inschakelen > Wijzigingen opslaan en sluiten) HP onderzoekt momenteel oplossingen voor toekomstige software releases.
Tijdens het beveiligingsproces Restore Identity (Identiteit herstellen) gaat de associatie met een virtueel token verloren.	Wanneer de gebruiker zijn of haar identiteit herstelt, verliest Credential Manager mogelijk de associatie met de locatie van het virtuele token bij het aanmeldscherm. Hoewel Credential Manager het virtuele token heeft geregistreerd, moet de gebruiker het token opnieuw registreren om de associatie te herstellen.	Momenteel is dit zo ontworpen. Wanneer Credential Manager wordt verwijderd zonder behoud van de identiteiten, wordt het systeemgedeelte (server) van het token vernietigd, zodat het token niet meer gebruikt kan worden voor aanmeldingen, zelfs als het clientgedeelte van het token wordt hersteld door de identiteit te herstellen. HP onderzoekt momenteel een lange-termijnoplossing.

Embedded Security for HP ProtectTools

Korte beschrijving	Meer informatie	Oplossing
Bij het coderen van mappen, submappen en bestanden op de PSD wordt een foutbericht weergegeven.	Als de gebruiker bestanden en mappen kopieert naar de PSD en de mappen, submappen of bestanden probeert te coderen, wordt het bericht Error Applying Attributes (Fout bij toepassen attributen) weergegeven. De gebruiker kan dezelfde bestanden coderen op de C:\-schijf, of op een extra geïnstalleerde vaste schijf.	Dit is zo ontworpen. Als bestanden of mappen naar de PSD worden verplaatst, worden ze automatisch gecodeerd. De bestanden of mappen hoeven dan ook niet "dubbel gecodeerd" te worden. Als wel wordt geprobeerd de bestanden dubbel te coderen met EFS op de PSD, wordt dit foutbericht weergegeven.
Kan geen eigenaar worden met een ander besturingssysteem op het MultiBoot platform.	Als een schijfeenheid is ingesteld voor het opstarten van meerdere besturingssystemen, kan alleen eigenaarschap worden verkregen met de Platform Initialization Wizard (Wizard platforminitialisatie) in een van de besturingssystemen.	Dit is zo ontworpen om beveiligingsredenen.
Een beheerder zonder de juiste rechten kan de inhoud van gecodeerde EFS-mappen bekijken en wissen, een nieuwe naam kan geven of de inhoud kan verplaatsen.	Het coderen van een map voorkomt niet dat een onbevoegde met beheerdersrechten de inhoud van gecodeerde EFS-mappen kan bekijken en wissen, een nieuwe naam kan geven of de inhoud kan verplaatsen.	Dit is zo ontworpen. Het is een EFS-voorziening en niet een voorziening van de geïntegreerde TPM-beveiligingschip. Embedded Security maakt gebruik van Microsoft EFS-software en EFS behoudt de toegangsrechten tot een bestand of map voor alle beheerders.
De gebruiker heeft geen mogelijkheid voor codering wanneer hij of zij probeert de vaste schijf te herstellen met FAT32.	Als de gebruiker probeert om de vaste schijf te herstellen met FAT32, zijn er geen mogelijkheden om bestanden of mappen te coderen met EFS.	Dit is zo ontworpen. Installeer geen software op een herstelde schijfeenheid met een FAT32-partitie. Microsoft EFS wordt alleen ondersteund op NTFS en kan niet worden uitgevoerd op FAT32. Dit is een voorziening van Microsoft EFS en staat los van de ProtectTools software.
De gebruiker kan het gearchiveerde XML-herstelbestand coderen of verwijderen.	De ACL's voor deze map zijn opzettelijk niet ingesteld. Hierdoor kan een gebruiker het bestand per ongeluk of opzettelijk coderen of verwijderen, waardoor het ontoegankelijk wordt. Nadat dit bestand is gecodeerd of verwijderd, kan niemand de TPM-software gebruiken.	Dit is zo ontworpen. Gebruikers hebben toegangsrechten voor een noodarchief, zodat zij de backup van hun Basic User Key kunnen opslaan/bijwerken. Gebruikers moeten worden geïnstrueerd nooit het gearchiveerde herstelbestand te coderen of te verwijderen.
Embedded Security EFS-interactie met Symantec Antivirus of Norton Antivirus resulteert in langere codering/decodering- en scantijden.	Gecodeerde bestanden verstoren de virusscan van Symantec Antivirus of Norton Antivirus 2005. Tijdens het scanproces wordt de gebruiker door de Basic User wachtwoordprompt ongeveer iedere tien bestanden om een wachtwoord gevraagd. Als de gebruiker geen wachtwoord invoert, loopt de Basic User wachtwoordprompt af, waardoor NAV2005 verder kan gaan met de scan. Wanneer Symantec Antivirus of Norton Antivirus een scan uitvoert, duurt het langer om bestanden te coderen met de Embedded Security EFS.	De gebruiker kan het coderingswachtwoord invoeren alvorens de scan te starten, of de bestanden decoderen, om de tijd die nodig is om Embedded Security EFS-bestanden te scannen te verkorten. De gebruiker kan Auto-Protect uitschakelen in Symantec Antivirus of Norton Antivirus, om de tijd die nodig is om gegevens te coderen/decoderen met Embedded Security EFS te verkorten.
Het archief voor noodherstel kan niet	Als de gebruiker een MultiMediaCard of Secure Digital-geheugenkaart (SD-geheugenkaart) plaatst tijdens het	Dit is zo ontworpen.

Korte beschrijving	Meer informatie	Oplossing
worden opgeslagen op verwijderbare media.	maken van het pad naar het archief voor noodherstel gedurende de initialisatie van Embedded Security, wordt een foutbericht weergegeven.	Het archief voor noodherstel kan niet worden opgeslagen op verwijderbare media. Het archief voor noodherstel kan worden opgeslagen op een netwerkschijf of op een andere lokale schijf die niet de C-schijf is.
Fouten doen zich voor nadat een spanningonderbreking de initialisatie van Embedded Security heeft onderbroken.	Als een spanningonderbreking zich voordoet tijdens het initialiseren van de geïntegreerde beveiligingschip, doet het volgende zich voor: - Als wordt geprobeerd de wizard Embedded Security Initialization (Initialisatie Embedded Security) te starten, wordt het volgende foutbericht weergegeven: The Embedded security cannot be initialized since the Embedded Security chip already has an Embedded Security owner. (Embedded Security kan niet worden geïnitieerd, omdat de geïntegreerde beveiligingschip al een Embedded Security eigenaar heeft.) - Als wordt geprobeerd de wizard Uzer Initialization (Gebruikerinitialisatie) te starten, wordt het volgende foutbericht weergegeven: The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first. (Embedded Security is niet geïnitieerd. Initialiseer Embedded Security om de wizard te gebruiken.)	Voer de volgende procedure uit om van de spanningonderbreking te herstellen:  OPMERKING: Gebruik de pijltoetsen om verschillende menu's en menu-items te selecteren en waarden te wijzigen (tenzij anders aangegeven). 1. Zet de computer aan of start deze opnieuw op. 2. Druk op F10 wanneer het bericht F10=Setup op het scherm wordt weergegeven. 3. Selecteer de gewenste taaloptie. 4. Druk vervolgens op enter. 5. Selecteer Security > Embedded Security (Beveiliging > Embedded Security). 6. Stel de optie Embedded security Device (Geïntegreerd apparaat) in op Enable (Inschakelen). 7. Druk op F10 om de wijziging te accepteren. 8. Selecteer File > Save changes and exit (Bestand > Wijzigingen opslaan en sluiten). 9. Druk vervolgens op enter. 10. Druk op F10 om de wijzigingen op te slaan en het hulpprogramma te sluiten.
Nadat de TPM-module is ingeschakeld, kan het wachtwoord voor het hulpprogramma Computer Setup (Computerinstellingen) (F10) worden verwijderd.	U heeft een wachtwoord voor het hulpprogramma Computer Setup (Computerinstellingen) (F10) nodig om de TPM-module in te schakelen. Wanneer de module is ingeschakeld, kan de gebruiker het wachtwoord verwijderen. Hierdoor kan iedereen met directe toegang tot het systeem de TPM-module herstellen, wat mogelijk gegevensverlies tot gevolg heeft.	Dit is zo ontworpen. Het wachtwoord voor het hulpprogramma Computer Setup (Computerinstellingen) (F10) kan alleen worden verwijderd door een gebruiker die het wachtwoord weet. HP raadt u echter ten eerste aan het hulpprogramma Computer Setup (Computerinstellingen) (F10) altijd met een wachtwoord te beschermen.
Het PSD-wachtwoordveld wordt niet meer weergegeven wanneer het systeem weer actief wordt vanuit de standbystand.	Wanneer een gebruiker zich bij het systeem aanmeldt nadat een PSD is gemaakt, vraagt de TPM om het Basic User wachtwoord. Als de gebruiker het wachtwoord niet invoert en het systeem overschakelt naar de standbystand, is het dialoogvenster voor het wachtwoord niet meer beschikbaar wanneer de gebruiker de computer weer activeert vanuit de standbystand.	Dit is zo ontworpen. Het PSD-wachtwoordveld verschijnt weer als de gebruiker zich afmeldt en weer aanmeldt.

Korte beschrijving	Meer informatie	Oplossing
Er is geen wachtwoord nodig om de Security Platform Policies te wijzigen.	Voor toegang tot Security Platform Policies (Beleid beveiligingsplatform) (zowel Machine (Apparaat) als User (Gebruiker)), hebben gebruikers met beheersrechten voor het systeem geen TPM-wachtwoord nodig.	Dit is zo ontworpen. Iedere beheerder kan Security Platform Policies (Beleid beveiligingsplatform) wijzigen, met of zonder TPM-gebruikerinitialisatie.
Wanneer een certificaat wordt bekeken, wordt het als onbetrouwbaar weergegeven.	Nadat HP ProtectTools is ingesteld en de wizard User Initialization (Gebruikerinitialisatie) is doorlopen, kan de gebruiker het uitgegeven certificaat bekijken. Wanneer het certificaat wordt bekeken, wordt het echter als onbetrouwbaar weergegeven. Het certificaat kan op dit moment worden geïnstalleerd door op de knop Install (Installeren) te klikken, maar hierdoor wordt het niet betrouwbaar.	Zelfondertekende certificaten zijn onbetrouwbaar. EFS-certificaten worden in een op de juiste manier geconfigureerde bedrijfsomgeving uitgegeven door een online certificeringsinstantie en zijn betrouwbaar.
Er doet zich een coderings- en decoderingsfout voor die slechts af en toe optreedt: The process cannot access the file because it is being used by another process. (Het proces kan geen toegang krijgen tot het bestand, omdat het door een ander proces wordt gebruikt.)	Deze fout treedt zelden op tijdens het coderen en decoderen van bestanden. De oorzaak is dat het bestand wordt gebruikt door een ander proces, hoewel dat bestand of die map niet wordt verwerkt door het besturingssysteem of andere applicaties.	U kunt dit als volgt oplossen: 1. Start het systeem opnieuw op. 2. Meld u af. 3. Meld u weer aan.
Als het opslagmedium wordt verwijderd voordat het genereren van nieuwe gegevens of de gegevensoverdracht is voltooid, kan dit resulteren in gegevensverlies.	Als opslagmedia zoals een MultiBay vaste schijf worden verwijderd, wordt de beschikbaarheid van de PSD nog steeds getoond en worden geen fouten gegenereerd tijdens het toevoegen/wijzigen van gegevens op de PSD. Nadat het systeem opnieuw is gestart, geeft de PSD veranderingen aan bestanden niet weer als die veranderingen gedaan zijn terwijl het verwijderbare opslagmedium niet beschikbaar was.	Verwijder een PSD niet voordat het genereren van gegevens of de gegevensoverdracht is voltooid. Dit probleem komt alleen voor als de gebruiker de PSD opent en vervolgens de vaste schijf verwijdert voordat het genereren van nieuwe gegevens of de gegevensoverdracht zij voltooid. Als de gebruiker toegang probeert te krijgen tot de PSD wanneer de verwijderbare vaste schijf niet aanwezig is, wordt het volgende foutbericht weergegeven: the device is not ready (het apparaat is niet klaar).
Als de gebruiker tijdens het ongedaan maken van de installatie de Basic User niet heeft geïnitieerd en het hulpmiddel Administration (Beheer) opent, is de optie Disable (Uitschakelen) niet beschikbaar en de installatie pas ongedaan worden gemaakt nadat Administration (Beheer) is gesloten.	De gebruiker kan bij het ongedaan maken van de installatie kiezen uit twee mogelijkheden: de TPM niet eerst uitschakelen; of de TPM wel eerst uitschakelen via het hulpprogramma Administration (Beheer). De Basic User Key moet zijn geïnitieerd om toegang te krijgen tot het hulpprogramma Administration (Beheer). Als de Basic User Key niet is geïnitieerd, zijn alle opties niet toegankelijk voor de gebruiker. Aangezien de gebruiker ervoor heeft gekozen het hulpprogramma Administration (Beheer) te openen (door op Yes (Ja) te klikken in het dialoogvenster met de tekst Click Yes to	Het hulpprogramma Administration (Beheer) wordt gebruikt om de TPM-beveiligingschip uit te schakelen. Die optie is echter niet beschikbaar als de Basic User Key nog niet is geïnitieerd. Als deze nog niet is geïnitieerd, selecteert u OK of Cancel (Annuleren) om verder te gaan met verwijderen.

Korte beschrijving	Meer informatie	Oplossing
	open Embedded Security Administration tool (Klik op Ja om het hulpprogramma Embedded Security Administration te openen), wordt met verwijderen gewacht totdat het hulpprogramma Administration (Beheer) is gesloten. Als de gebruiker in dat dialoogvenster op No (Nee) klikt, wordt het hulpprogramma Administration (Beheer) helemaal niet geopend en wordt doorgegaan met het ongedaan maken van de installatie.	
Als een PSD is gemaakt op 2 gebruikersaccounts en snelle gebruikerswisseling wordt gebruikt in 128-MB systeemconfiguraties, loopt het systeem soms vast.	Het systeem loopt mogelijk vast (het scherm wordt zwart en het toetsenbord en de muis reageren niet meer) in plaats van het welkomstschermb (aanmeldscherm) weer te geven bij gebruik van fast-switching met een minimaal RAM.	Waarschijnlijk wordt dit veroorzaakt door een probleem met de timing bij lage geheugenconfiguraties. Geïntegreerde graphics maken gebruik van een UMA-architectuur en 8 MB geheugen. Hierdoor blijft slechts 120 MB beschikbaar voor de gebruiker. De fout wordt gegenereerd wanneer deze 120 MB wordt gedeeld door beide gebruikers die zich hebben aangemeld en gebruikmaken van snelle gebruikerswisseling. Dit kunt u vermijden door het systeem opnieuw op te starten en de geheugenconfiguratie uit te breiden (HP levert geen 128-MB configuraties bij beveiligingsmodules).
EFS User Authentication (EFS-gebruikerverificatie) (wachtwoordverzoek) loopt af met access denied (Toegang geweigerd).	Het wachtwoordschermb EFS User Authentication (EFS-gebruikerverificatie) wordt opnieuw geopend nadat de gebruiker op OK klikt of het systeem activeert vanuit de standbystand.	Dit is zo ontworpen. Een timer van 30 seconden is ingesteld die het foutbericht genereert, om problemen met Microsoft EFS te voorkomen.
In functionele beschrijvingen is minimale afbreking waargenomen tijdens het instellen van Japans.	Functionele beschrijvingen tijdens standaardinstallatie met de installatiewizard worden afgebroken.	HP zal dit in een volgende release corrigeren.
EFS-codering werkt ook als geen wachtwoord wordt ingetypt wanneer daarom wordt gevraagd.	Als u de vraag voor een gebruikerswachtwoord laat aflopen, kunt u nog altijd een bestand of map coderen.	Wachtwoordverificatie is niet nodig om bestanden en mappen te coderen, omdat dit een voorziening is van de Microsoft EFS-codering. Voor decodering is in dit geval het gebruikerswachtwoord nodig.
Beveiligde e-mail wordt ondersteund, zelfs wanneer beveiligde e-mail niet is gespecificeerd in de wizard User Initialization (Gebruikerinitialisatie) of beveiligde e-mail is uitgeschakeld onder het gebruikersbeleid.	Geïntegreerde beveiligingssoftware en de wizard hebben geen invloed op de instellingen van een e-mailclient (Outlook, Outlook Express, of Netscape).	Dit is zo ontworpen. De configuratie van TPM e-mailinstellingen voorkomt het direct wijzigen van coderinginstellingen in een e-mailclient niet. Gebruik van beveiligde e-mail wordt ingesteld en beheerd door applicaties van derden. Met de HP wizard kunt u een koppeling maken met de drie referentieapplicaties om deze direct aan uw wensen aan te passen.
Als een tweede keer op dezelfde computer of op een eerder geïnitieerde computer grootschalige implementatie wordt uitgevoerd, worden Emergency Recovery	Als u twee keer grootschalige implementatie uitvoert op een willekeurig HP ProtectTools Embedded Security systeem, worden bestaande Recovery Archives (Herstelarchieven) en Recovery Tokens (Hersteltokens) nutteloos door het overschrijven van de XML-bestanden.	HP werkt momenteel aan een oplossing voor het overschrijven van de XML-bestanden en zal in een toekomstig SoftPaq een oplossing bieden.

Korte beschrijving	Meer informatie	Oplossing
(Noodherstel) en Emergency Token (Noodtoken) bestanden overschreven. De nieuwe bestanden kunnen niet voor herstel worden gebruikt.		
Automatische aanmeldscripts werken niet wanneer een gebruiker wordt hersteld in Embedded Security.	De fout treedt op nadat de gebruiker de volgende acties uitvoert: - Eigenaar en gebruiker initialiseren in Embedded Security (waarbij gebruikgemaakt wordt van de standaardlocatie Mijn documenten). - De chip naar de fabrieksinstellingen in het BIOS herstellen. - Computer opnieuw opstarten. - Beginnen met het herstellen van Embedded Security. Tijdens het herstelproces vraagt Credential Manager of het systeem de aanmeldingsgegevens kan onthouden voor Infineon TPM User Authentication. Als de gebruiker Yes (Ja) selecteert, wordt de locatie van SPemRecToken automatisch weergegeven in het tekstvak. Hoewel deze locatie juist is, wordt het volgende foutbericht weergegeven: No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from. (Geen token voor noodherstel opgegeven. Selecteer de locatie waar het token kan worden opgehaald.)	Klik op de knop Browse (Bladeren) op het scherm om de locatie te selecteren. Het herstelproces wordt vervolgd.
PSD's voor meerdere gebruikers functioneren niet in een omgeving die gebruikmaakt van snelle gebruikerswisseling.	Deze fout treedt op wanneer meerdere gebruikers zijn gemaakt en een PSD toegewezen hebben gekregen met dezelfde schijffletter. Als gebruikers vervolgens proberen snelle gebruikerswisseling te gebruiken wanneer de PSD is geladen, is de PSD van de tweede gebruiker niet beschikbaar.	De PSD van de tweede gebruiker wordt alleen beschikbaar als deze opnieuw wordt geconfigureerd en een andere schijffletter wordt gebruikt, of als de eerste gebruiker zich afmeldt.
De PSD is uitgeschakeld en kan na het formatteren van de vaste schijf waarop de PSD is gegenereerd niet worden gewist.	Het pictogram van de PSD is nog zichtbaar, maar het foutbericht drive is not accessible (Schijf is niet toegankelijk) wordt weergegeven wanneer de gebruiker probeert toegang te krijgen tot de PSD. De gebruiker kan de PSD niet wissen en het volgende bericht wordt weergegeven: your PSD is still in use, please be sure that your PSD contains	Dit is zo ontworpen. Als een klant de opslaglocatie van de PSD-gegevens wist, of de verbinding ermee verbreekt, blijft de Embedded Security PSD-schijfemulatie in werking en produceert fouten door gebrek aan communicatie met de ontbrekende gegevens. Oplossing: Nadat de computer weer opnieuw is opgestart, zullen de emulaties niet worden geladen en kan de gebruiker de oude PSD-emulatie verwijderen en een nieuwe PSD maken.

Korte beschrijving	Meer informatie	Oplossing
	no open files and is not accessed by another process (Uw PSD is nog in gebruik. Sluit alle geopende bestanden op uw PSD en controleer of de PSD niet wordt gebruikt door een ander proces). De gebruiker moet het systeem opnieuw opstarten om de PSD te wissen en het wordt na het opnieuw opstarten niet geladen.	
Een interne fout wordt gedetecteerd wanneer de gebruiker herstelt vanuit het Automatic Backup Archive (Archief voor automatische backup).	Als de gebruiker in Embedded Security op de optie Restore under Backup (Herstellen onder backup) klikt om te herstellen vanuit het archief met automatische backups en vervolgens SPSystemBackup.xml selecteert, zal de wizard Herstellen niet kunnen worden uitgevoerd en zal het volgende foutbericht worden weergegeven: The selected Backup Archive does not match the restore reason. Please select another archive and continue. (Het geselecteerde backuparchief komt niet overeen met de reden voor herstellen. Selecteer een ander archief en ga door.)	Als de gebruiker SpSystemBackup.xml selecteert wanneer SpBackupArchive.xml nodig is, kan de wizard Embedded Security niet worden uitgevoerd en zal het volgende bericht worden weergegeven: An internal Embedded Security error has been detected (Er is een interne Embedded Security fout gedetecteerd). De gebruiker moet het juiste XML-bestand selecteren voor de vereiste reden. De processen werken zoals ontworpen en op een juiste manier. Het interne Embedded Security foutbericht is echter niet duidelijk. Het zou een duidelijkere boodschap moeten weergeven. HP werkt aan verbetering hiervan voor toekomstige producten.
Het beveiligingssysteem vertoont bij meerdere gebruikers een herstelfout.	Als de beheerder tijdens het herstelproces gebruiker selecteert om te herstellen, kunnen de gebruikers die niet worden geselecteerd hun sleutels niet herstellen, wanneer zij op een later tijdstip een herstelactie proberen uit te voeren. Het foutbericht decryption process failed (Coderen mislukt) wordt weergegeven.	De niet-geselecteerde gebruikers kunnen worden hersteld door de TPM te herstellen, het herstelproces uit te voeren en vervolgens alle gebruikers te selecteren voor de volgende standaard dagelijkse backup wordt uitgevoerd. Als de automatische backup wordt uitgevoerd, overschrijft deze de niet-herstelde gebruikers en gaan hun gegevens verloren. Als een nieuwe backup van het systeem wordt opgeslagen, kunnen de gebruikers die eerder niet werden geselecteerd niet worden hersteld. De gebruiker moet ook de gehele systeembackup herstellen. Een backup van het archief kan apart worden opgeslagen.
Als u de standaardinstellingen voor het systeem-ROM herstelt, wordt de TPM verborgen.	Als u de standaardinstellingen voor het systeem-ROM herstelt, wordt de TPM verborgen voor Windows. Hierdoor kan de beveiligingssoftware niet goed worden uitgevoerd en worden de gegevens die met behulp van de TPM zijn gecodeerd ontoegankelijk.	TPM beschikbaar maken in het BIOS: Open het hulpprogramma Computer Setup (Computerinstellingen) (f10) en navigeer naar Security > Device security (Beveiliging > Apparaatbeveiliging). Wijzig vervolgens het veld van Hidden (Verbergen) naar Available (Beschikbaar).
Automatische backup kan niet worden uitgevoerd voor de aangegeven schijf eenheid.	Wanneer een beheerder Automatic Backup (Automatische backup) instelt in Embedded Security, wordt een ingang gemaakt in Windows > Tasks > Scheduled Task (Windows > Taken > Geplande taak). Deze geplande taak in Windows wordt zo geconfigureerd dat NT AUTHORITY\SYSTEM wordt gebruikt voor rechten om de backup uit te voeren. Dit werkt voor alle lokale schijf eenheden op een juiste manier.	U kunt dit omzeilen door NT AUTHORITY\SYSTEM te wijzigen in (computernaam)\(naam beheerder). Dit is de standaardinstelling voor als de geplande taak handmatig wordt gemaakt. HP werkt momenteel aan toekomstige productreleases met standaardinstellingen die computernaam\naam beheerder bevatten.

Korte beschrijving	Meer informatie	Oplossing
	Als de beheerder Automatic Backup (Automatische backup) configureert zodat de backup wordt opgeslagen op een bepaalde schijf eenheid, kan het proces niet worden voltooid, omdat NT AUTHORITY\SYSTEM geen rechten heeft om de ingestelde schijf eenheid te gebruiken. Als de automatische backup is gepland om te worden gemaakt zodra men zich aanmeldt, geeft het pictogram van Embedded Security in het systeemvak rechtsonder op de taakbalk het volgende bericht weer: The Backup Archive location is currently not accessible. Click here if you want to backup to a temporary archive until the Backup Archive is accessible again. (De locatie voor de automatische backup is op dit moment niet beschikbaar. Klik hier om een backup te maken naar een tijdelijk archief totdat het backuparchief weer toegankelijk is.) Als de automatische backup is gepland voor een bepaalde tijd, wordt de backup niet voltooid en wordt geen foutbericht weergegeven.	
Embedded Security kan niet tijdelijk worden uitgeschakeld in het Embedded Security GUI.	De huidige 4.0-software is ontworpen voor HP Notebook 1.1B implementaties en ondersteunt ook HP Desktop 1.2 implementaties. De mogelijkheid om dit uit te schakelen wordt nog altijd ondersteund in de software-interface voor TPM 1.1-platforms.	HP zal dit in een volgende release corrigeren.

Device Access Manager for HP ProtectTools

Korte beschrijving	Gegevens	Oplossing
Gebruikers krijgen geen toegang tot apparaten binnen Device Access Manager, maar de apparaten zijn nog altijd toegankelijk.	Eenvoudige configuratie en/of Apparaatklasse configureren zijn gebruikt binnen Device Access Manager om gebruikers toegang tot apparaten te weigeren. Ondanks dat de gebruikers geen toegang hebben, kunnen zij nog altijd bij alle apparaten.	Controleer of de service HP ProtectTools Device Locking is gestart. Als beheerder bladert u naar Configuratiescherm > Systeembeheer > Services . Zoek in het venster Services naar de service HP ProtectTools Device Locking/Auditing . Zorg ervoor dat de service wordt gestart en het opstarttype is ingesteld op Automatisch .
Een gebruiker heeft onverwacht (geen) toegang tot een apparaat.	Device Access Manager is gebruikt om gebruikers toegang tot bepaalde apparaten te weigeren en juist toegang te geven tot andere apparaten. Wanneer gebruikers gebruikmaken van het systeem, hebben zij toegang tot apparaten waarvan zij denken dat zij er geen toegang toe hebben, en geen toegang tot apparaten waartoe zij juist wel toegang zouden moeten hebben.	Controleer met Apparaatklasse configureren binnen Device Access Manager de apparaatinstellingen voor de gebruikers. Selecteer Security Manager > Device Access Manager > Apparaatklasse configureren . Open de niveaus in de boomstructuur van Device Class (Apparaatklasse) en bekijk de instellingen die van toepassing zijn op de gebruiker. Controleer of er toestemmingen op "Weigeren" staan waartoe de gebruiker of Windows-groep (bijvoorbeeld Gebruikers, Administrators) waarvan de gebruiker lid is, toegang zou moeten hebben.
Toestaan of weigeren – wat heeft voorrang?	Binnen Apparaatklasse configureren is de volgende configuratie ingesteld: Toestaan is toegekend aan een Windows-groep (bijvoorbeeld BUILTIN\Administrators) en Weigeren is toegekend aan een andere Windows-groep (bijvoorbeeld BUILTIN\Gebruikers) op hetzelfde niveau in de apparaatklassehiërarchie (bijvoorbeeld Dvd/cd-rom-drives). Als een gebruiker lid is van beide groepen (bijvoorbeeld Beheerder), welke heeft dan voorrang?	De gebruiker wordt de toegang tot het apparaat geweigerd. Weigeren heeft voorrang boven Toestaan. Toegang wordt geweigerd op basis van de manier waarop Windows de effectieve toegang voor het apparaat bepaalt. Eén groep wordt toegang geweigerd en één groep krijgt wel toegang, maar de gebruiker is lid van beide groepen. De gebruiker wordt toegang geweigerd, omdat het weigeren van toegang voorrang heeft boven het verlenen van toegang. U kunt dit omzeilen door de groep Gebruikers toegang te weigeren op het niveau Dvd/cd-rom-drives en Administrators toegang te verlenen op het niveau onder Dvd/cd-rom-drives. U kunt bijvoorbeeld ook bepaalde Windows-groepen definiëren: één zonder toegang tot dvd/cd-rom-drives en één met toegang tot dvd/cd-rom-drives. Vervolgens kunnen specifieke gebruikers worden toegevoegd aan de juiste groep.

Overige problemen

Invloed op software — korte beschrijving	Meer informatie	Oplossing
Security Manager — waarschuwing ontvangen: The security application can not be installed until the HP Protect Tools Security Manager is installed (De beveiligingsapplicatie kan niet worden geïnstalleerd voordat HP ProtectTool Security Manager is geïnstalleerd).	Alle beveiligingsapplicaties zoals Embedded Security, Java Card Security en biometrische lezers zijn uitbreidbare invoegtoepassingen voor de interface van Security Manager. Security Manager moet zijn geïnstalleerd voordat een beveiligingsinvoegtoepassing die is goedgekeurd door HP kan worden geladen.	De Security Manager software moet zijn geïnstalleerd voordat u een beveiligingsinvoegtoepassing installeert.
Hulpprogramma TPM Firmware Update voor modellen met TPM's die geschikt zijn voor Broadcom, het hulpprogramma dat wordt geboden via de HP ondersteuningswebsite, geeft het volgende bericht weer: ownership required (Eigendom noodzakelijk).	Dit is het verwachte gedrag van TPM-firmwarehulpprogramma's voor modellen met TPM's die geschikt zijn voor Broadcom. Met het hulpprogramma voor de firmware-upgrade kan de gebruiker de firmware upgraden, met of zonder een endorsement key (EK). Als er geen EK beschikbaar is, is geen verificatie vereist om de firmware-upgrade te voltooien. Als er een EK beschikbaar is, moet een TPM-eigenaar bestaan, aangezien verificatie door de eigenaar is vereist voor de upgrade. Nadat de upgrade is voltooid, moet het platform opnieuw worden opgestart om de nieuwe firmware in werking te stellen. Als de BIOS-TPM wordt hersteld naar de fabrieksinstellingen, wordt het eigenaarschap verwijderd en kan de firmware niet worden geüpgraded totdat het Embedded Security softwareplatform en de wizard User Initialization (Gebruikerinitialisatie) zijn geconfigureerd.	1. Installeer de Embedded Security software opnieuw. 2. Voer de wizard Platform and User Configuration (Configuratie platform en gebruiker) uit. 3. Zorg ervoor dat Microsoft .NET framework 1.1 op het systeem is geïnstalleerd: a. Klik op Start. b. Klik op Configuratiescherm. c. Klik op Software. d. Controleer of Microsoft .NET framework 1.1 in de lijst staat. 4. Controleer de hardware- en softwareconfiguratie: a. Klik op Start. b. Klik op Alle programma's. c. Klik op HP ProtectTools Security Manager. d. Selecteer Geïntegreerde beveiliging in de boomstructuur. e. Klik op More Details (Meer informatie). Het systeem zou als volgt geconfigureerd moeten zijn: • Product version = V4.0.1 (Productversie = V4.0.1) • Embedded Security State (Status Embedded Security): Chip State = Enabled, Owner State = Initialized, User State = Initialized (Chipstatus = Ingeschakeld, Eigenaarstatus = Geïntialiseerd, Gebruikerstatus = Geïntialiseerd)



OPMERKING: U wordt aangeraden uw systeem altijd opnieuw op te starten nadat een firmware-update is uitgevoerd. De firmwareversie wordt pas juist geïdentificeerd wanneer het systeem opnieuw is opgestart.

Invloed op software — korte beschrijving	Meer informatie	Oplossing
		• Component Info (Onderdeelinformatie): TCG Spec. Version = 1.2 (TCG spec. versie = 1.2) • Vendor = Broadcom Corporation (Leverancier = Broadcom Corporation) • FW Version = 2.18 (or greater) (Firmwareversie = 2.18 (of hoger)) • TPM Device driver library version 2.0.0.9 (or greater) (TPM-apparaatstuurprogramma library versie 2.0.0.9 (of hoger)) 5. Als uw firmwareversie niet versie 2.18 is, downloadt en updatet u de TPM-firmware. De SoftPaq TPM firmware is een ondersteuningsdownload die beschikbaar is op de website van HP: http://www.hp.com.
HP ProtectTools Security Manager: soms wordt bij het afsluiten van de Security Manager interface een foutbericht weergegeven.	Af en toe (1 op de 12 gebeurtenissen), wordt een foutbericht weergegeven wanneer u op de knop Sluiten in de rechterbovenhoek van het scherm klikt om Security Manager af te sluiten voordat alle invoegtoepassingen volledig zijn geladen.	Dat komt door timing-afhankelijkheid van de laadtijd van invoegtoepassingen bij het afsluiten en opnieuw starten van Security Manager. Aangezien PTHOST.exe de shell is waarin de andere applicaties (invoegtoepassingen) worden uitgevoerd, is het afhankelijk van de invoegtoepassing of de laadtijd wordt voltooid (services). Deze fout wordt gegenereerd wanneer u de shell sluit voordat de invoegtoepassing volledig is geladen. Wacht tot in Security Manager het bericht Services loading (Services worden geladen) niet langer bovenin het Security Manager venster wordt weergegeven en alle invoegtoepassingen in de linkerkolom worden weergegeven. Geef de invoegtoepassingen genoeg tijd om te laden, om fouten te voorkomen.
HP ProtectTools: onbeperkte toegang of onbeperkte beheerdersrechten vormen een beveiligingsrisico.	Als de clientcomputer onbeperkt toegankelijk is, loopt u een aanzienlijk beveiligingsrisico op onder andere de volgende gebieden: • PSD wissen • Kwaadwillige wijzigingen in gebruikersinstellingen • Beveiligingsbeleid en -functies uitschakelen	Beheerders wordt aangeraden “best practices” aan te houden bij het beperken van de rechten van eindgebruikers en gebruikerstoegang. Geef onbevoegden geen beheerdersrechten.
De wachtwoorden voor het BIOS en Embedded Security van het besturingssysteem zijn niet gesynchroniseerd.	Als een gebruiker een nieuw wachtwoord niet valideert als het BIOS Embedded Security wachtwoord, wordt het BIOS Embedded Security wachtwoord hersteld naar het oorspronkelijke wachtwoord van Embedded Security via f10 BIOS.	Dit is zo ontworpen. Deze wachtwoorden kunnen opnieuw worden gesynchroniseerd door het Basic User wachtwoord voor het besturingssysteem te wijzigen en het bij de wachtwoordprompt voor BIOS Embedded Security te verifiëren.
Nadat verificatie voor het opstarten is ingeschakeld in het BIOS, kan slechts	De TPM BIOS-pincode wordt geassocieerd met de eerste gebruiker die de gebruikersinstellingen initialiseert. Als een computer meerdere gebruikers	Dit is zo ontworpen. HP adviseert de IT-afdeling van de klant aan om een goed beveiligingsbeleid te voeren bij de implementatie van de beveiligingsoplossing, en ervoor te zorgen dat het wachtwoord voor de BIOS-

Invloed op software — korte beschrijving	Meer informatie	Oplossing
één gebruiker zich bij het systeem aanmelden.	heeft, is de eerste gebruiker in principe de beheerder. De eerste gebruiker zal zijn of haar TPM-gebruikerspincode aan andere gebruikers moeten geven, zodat zij deze kunnen gebruiken om zich aan te melden.	beheerder wordt geconfigureerd door IT-beheerders voor beveiliging op systeemniveau.
Nadat de TPM-fabrieksinstellingen zijn hersteld, moet de gebruiker zijn of haar pincode wijzigen om ervoor te zorgen dat TPM-verificatie voor het opstarten werkt.	Nadat een herstelactie is uitgevoerd, moet de gebruiker zijn of haar pincode wijzigen of een nieuwe gebruiker aanmaken om zijn of haar gebruikersinstellingen te initialiseren zodat TPM BIOS-verificatie werkt. Er is geen optie om TPM BIOS-verificatie te activeren.	Dit is zo ontworpen. Een herstelactie waarbij de fabrieksinstellingen worden hersteld wist de Basic User Key. De gebruiker moet zijn of haar pincode wijzigen of een nieuwe gebruiker aanmaken om de Basic User Key opnieuw te initialiseren.
Ondersteuning voor verificatie bij opstarten is niet standaard ingesteld bij gebruik van Reset to Factory Settings (Fabrieksinstellingen herstellen) in Embedded Security.	In Computer Setup (Computerinstellingen) wordt de optie Ondersteuning voor verificatie bij opstarten niet hersteld naar de fabrieksinstellingen bij gebruik van de optie Reset to Factory Settings (Fabrieksinstellingen herstellen) in Embedded Security Device. Ondersteuning voor verificatie bij opstarten is standaard ingesteld op Disable (Uitschakelen).	Met de optie Reset to Factory Settings (Fabrieksinstellingen herstellen) kunt u Embedded Security Device uitschakelen, waarmee u de andere opties van Embedded Security (waaronder Ondersteuning voor verificatie bij opstarten) worden verborgen. Nadat Embedded Security Device weer is ingeschakeld, blijft Ondersteuning voor verificatie bij opstarten ingeschakeld. HP werkt momenteel aan een oplossing die in een toekomstige web-based ROM SoftPak zal worden aangeboden.
Opstartverificatie overlapt tijdens het opstartproces met het BIOS-wachtwoord.	De gebruiker wordt tijdens de opstartverificatie gevraagd zich bij het systeem aan te melden met het TPM-wachtwoord, maar als de gebruiker op F10 drukt om toegang te krijgen tot het BIOS, krijgt de gebruiker alleen leesrechten.	De gebruiker moet in plaats van het TPM-wachtwoord het BIOS-wachtwoord typen in het venster voor opstartverificatie, om naar het BIOS te kunnen schrijven.
Het BIOS vraagt nadat het Eigenaarswachtwoord is gewijzigd om zowel het oude als het nieuwe wachtwoord via Computer Setup (Computerinstellingen).	Het BIOS vraagt om zowel het oude als het nieuwe wachtwoord via Computer Setup (Computerinstellingen) nadat het Eigenaarswachtwoord is gewijzigd in de Windows-software van Embedded Security.	Dit is zo ontworpen. Dit wordt veroorzaakt doordat het BIOS niet met de TPM kan communiceren om het TPM-wachtwoord te controleren als het besturingssysteem wordt uitgevoerd.

Woordenlijst

Archief voor noodherstel Een beschermde opslagplaats waarmee Basic User Keys opnieuw kunnen worden gecodeerd van de ene Platform Owner Key naar de andere.

Automatic DriveLock Een beveiligingsvoorziening waarmee DriveLock wachtwoorden automatisch worden gegenereerd en beschermd door de geïntegreerde TPM-beveiligingschip. Als de gebruiker tijdens het opstarten door de geïntegreerde TPM-beveiligingschip is geverifieerd door het juiste TPM Basic User Key-wachtwoord in te voeren, wordt de vaste schijf in het BIOS vrijgegeven aan de gebruiker.

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

BIOS-beveiligingsmodus Een instelling in Java Card Security voor gebruikersverificatie door middel van een Java Card en een geldige pincode.

BIOS-profiel Een verzameling configuratie-instellingen van het BIOS die kunnen worden opgeslagen en worden toegepast op andere accounts.

Certificeringsinstantie Een organisatie die de certificaten uitdeeft die nodig zijn voor een public key infrastructure.

Coderen Een cryptografische procedure, zoals het gebruik van een algoritme, die wordt gebruikt om platte tekst om te zetten in gecijferde tekst, zodat niet-gemachtigde ontvangers de gegevens niet kunnen lezen. Er zijn vele manieren voor het coderen van gegevens, die de basis vormen van netwerkbeveiliging. Veelvoorkomende coderingsmethoden zijn Data Encryption Standard en codering door middel van publieke sleutels.

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

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

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

Digitaal certificaat Elektronische referenties waarmee de identiteit van een persoon of bedrijf wordt bevestigd, door de identiteit van de certificaateigenaar te koppelen aan een paar elektronische sleutels waarmee digitale informatie wordt ondertekend.

Digitale handtekening Gegevens die met een bestand worden meegestuurd om te bevestigen wie de afzender is en dat het bestand niet is gewijzigd na de ondertekening.

Domein Een verzameling computers die deel uitmaken van een netwerk en gebruikmaken van een gezamenlijke directorydatabase. Elk domein heeft een unieke naam en een reeks eigen regels en procedures.

DriveLock Een beveiligingsvoorziening waarmee de vaste schijf aan een gebruiker wordt gekoppeld. Deze moet bij het opstarten van de computer het juiste DriveLock wachtwoord opgeven.

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

Identiteit Een verzameling referenties en instellingen in de HP ProtectTools Credential Manager, die wordt behandeld als een account of profiel van een bepaalde gebruiker.

Java Card Een klein hardwareapparaat met het formaat van een bankpas, waarop identificatiegegevens van de eigenaar zijn opgeslagen. Deze kunnen worden gebruikt voor verificatie op een computer.

Migratie Een taak waarmee het beheren, herstellen en overzetten van sleutels en certificaten wordt uitgevoerd.

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

Opnieuw opstarten Het opnieuw opstarten van de computer.

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

Personal Secure Drive (PSD) Biedt een beveiligde opslagruimte voor gevoelige informatie.

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

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

Single Sign On Een voorziening waarmee referenties worden opgeslagen en de Credential Manager kan worden gebruikt voor toegang tot internet en Windows-applicaties waarvoor wachtwoordverificatie vereist is.

Smart Card Een klein hardwareapparaat met het formaat van een bankpas, waarop identificatiegegevens van de eigenaar zijn opgeslagen. Deze kunnen worden gebruikt voor verificatie op een computer.

Strengere beveiliging Een beveiligingsvoorziening in BIOS Configuration die betere beveiliging mogelijk maakt van de opstart- en beheerderswachtwoorden en andere vormen van opstartverificatie.

Trusted Platform Module (TPM) geïntegreerde beveiligingschip (alleen bepaalde modellen) Een geïntegreerde beveiligingschip die zeer gevoelige gebruikersgegevens beschermt tegen kwaadwillende aanvallers. Dit is de vertrouwensbasis voor een bepaald platform. De TPM biedt cryptografische algoritmen en acties die voldoen aan de specificaties van de Trusted Computing Group (TCG).

USB-token Een beveiligingsapparaat waarop identificatiegegevens van een gebruiker worden opgeslagen. Dit apparaat wordt net als een Java Card of biometrische lezer gebruikt om de eigenaar van een computer te verifiëren.

Verificatie Het controleren of een gebruiker gemachtigd is om een taak uit te voeren, zoals toegang krijgen tot een computer, instellingen voor een bepaald programma wijzigen of beveiligde gegevens bekijken.

Virtueel token Een virtueel token werkt ongeveer op dezelfde manier als een Java Card en kaartlezer. Het token wordt opgeslagen op de vaste schijf van de computer of in het register van Windows. Wanneer u zich aanmeldt met een virtueel token, wordt u om een gebruikerspincode gevraagd om de verificatie te voltooien.

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

Index

A

Account
 basisgebruiker 31
 Credential Manager 15
Achtergrondservice, Device Access
 Manager 54
Apparaatopties 44
Automatic DriveLock 48

B

Backup maken en herstellen
 certificeringsinformatie 34
 Embedded Security 34
 HP ProtectTools modules 9
 Single Sign On gegevens 21
Basic User Key, wachtwoord
 instellen 31
 wijzigen 33
Basisgebruikersaccount 31
Beheerderstaken
 Credential Manager 25
 Java Card 39
Beheren, toegang tot
 apparatuur 53
Belangrijkste
 beveiligingsdoelstellingen 5
Beperken
 toegang tot apparatuur 53
 toegang tot gevoelige
 gegevens 5
Beveiliging
 belangrijkste doelstellingen 5
 rollen 7
Beveiligingsrollen 7
Biometrische lezers 15
BIOS-beheerder, wachtwoord 8
BIOS Configuration for HP
 ProtectTools
 Automatic DriveLock 48

instellingen aanvullende module
 beheren 47
instelwachtwoord, instellen 49
instelwachtwoord, wijzigen 50
opstartopties 44
opstartverificatie 47
opstartverificatie bij opnieuw
 opstarten Windows 50
opstartwachtwoord,
 instellen 49
opstartwachtwoord,
 wijzigen 49
Smart Card,
 opstartverificatie 47
strengere beveiliging 50
systeemconfiguratie,
 opties 44
wachtwoordopties,
 instellen 50
BIOS-instelwachtwoord
 instellen 49
 wijzigen 50

C

Coderen
 gebruikers 61
 gebruikersverificatie 61
 methoden 60
Coderen, bestanden en
 mappen 32
Coderen, schijf 59
Computer Setup
 (Computerinstellingen)
 beheerderwachtwoord 8
 wachtwoord, instellen 49
 wachtwoord, wijzigen 50
 wachtwoorden, beheren 48
Computer Setup
 (Computerinstellingen),
 wachtwoord 8
Credential Manager for HP
 ProtectTools
 aangepaste
 verificatievereisten 25
 aanmelden 14
 aanmeldingswachtwoord 7
 aanmeldingswizard 14
 aanmeldspecificaties 25
 account, toevoegen 19
 account, verwijderen 19
 andere referenties
 registreren 16
 applicatiebescherming 23
 applicatiebescherming,
 opheffen 23
 beheerderstaken 25
 beperken,
 applicatietoegang 23
 gebruikerverificatie 27
 identiteit 18
 identiteit, verwijderen 18
 identiteit, wissen 18
 instellingen, configureren 26
 instelprocedures 14
 nieuwe account,
 aankomen 15
 problemen oplossen 66
 referentie, eigenschappen
 configureren 26
 referenties, registreren 15
 registreren, Java Card 15
 registreren, token 15
 registreren, virtueel token 15
 Single Sign On (SSO) 20
 SSO, automatische
 registratie 20
 SSO, handmatige
 registratie 21

- SSO-applicatie, eigenschappen wijzigen 21
- SSO-applicatie, exporteren 21
- SSO-applicatie, importeren 22
- SSO-applicatie, verwijderen 21
- SSO-applicaties en referenties 21
- SSO nieuwe applicatie 20
- SSO-referenties, wijzigen 22
- tokenpincode, wijzigen 18
- USB-eToken, registreren 16
- vastleggen, vingerafdrukken 15
- vergrendelen, computer 18
- vingerafdruk, aanmelden 15
- vingerafdruklezer 15
- virtueel token, aanmaken 17
- wachtwoord herstelbestand 8
- wijzigen, instellingen voor applicatiebescherming 24
- Windows, aanmelden 19
- Windows-aanmeldingswachtwoord, wijzigen 17
- Windows Logon (Windows-aanmelding), toestaan 27

D

- Device Access Manager for HP ProtectTools
 - achtergrondservice 54
 - apparaat, toegang verlenen aan één 57
 - apparaatklasse, configuratie 56
 - apparaatklasse, toegang verlenen aan één 57
 - eenvoudige configuratie 55
 - gebruiker of groep, toegang weigeren 56
 - gebruiker of groep, toevoegen 56
 - gebruiker of groep, verwijderen 56
 - problemen oplossen 76
- Doelstellingen, beveiliging 5
- Drive Encryption for HP ProtectTools
 - coderen, schijf 60

- codering wijzigen 60
- Drive Encryption
 - herstelservice 63
- Drive Encryption sleutels 63
- gebruiker, verwijderen 61
- gebruiker toevoegen 61
- instellen, wachtwoord 61
- schijf decoderen 60
- token wijzigen 61
- verificatie wijzigen 61

E

- Eigenaarswachtwoord
 - definitie 8
 - instellen 30
 - wijzigen 34
- Eigenschappen
 - applicatie 21
 - referentie 26
 - verificatie 25
- Embedded Security for HP ProtectTools
 - backupbestand, maken 34
 - Basic User Key 31
 - Basic User Key, wachtwoord wijzigen 33
 - basisgebruikersaccount 31
 - blijvend uitschakelen 35
 - certificeringsgegevens, herstellen 34
 - coderen, bestanden en mappen 32
 - eigenaarswachtwoord, wijzigen 34
 - gecodeerde e-mail 32
 - herstellen, gebruikerswachtwoord 34
 - in- en uitschakelen 34
 - initialiseren, chip 30
 - inschakelen, TPM-beveiligingschip 30
 - instelprocedures 30
 - migreren, sleutels 35
 - Personal Secure Drive 32
 - problemen oplossen 69
 - wachtwoord 8
 - weer inschakelen na blijvend uitschakelen 35

G

- Geavanceerde taken
 - BIOS Configuration 47
 - Credential Manager 25
 - Device Access Manager 56
 - Embedded Security 34
 - Java Card 39
- Gegevens, toegang beperken 5
- Geïntegreerde beveiligingschip initialiseren 30
- Gerichte diefstal, bescherming bieden tegen 5

H

- Herstellen, gecodeerde gegevens 63
- HP ProtectTools, voorzieningen 2
- HP ProtectTools Backup en herstellen 9
- HP ProtectTools Security, toegang 4

I

- Identiteit, beheren
 - Credential Manager 18
- Identiteit, verwijderen
 - Credential Manager 18
- Inschakelen
 - apparaatopties 44
 - Automatic DriveLock 48
 - Embedded Security 34
 - Embedded Security weer inschakelen na blijvend uitschakelen 35
 - Java Card, opstartverificatie 40
 - opstartverificatie 47
 - strengere beveiliging 50
 - TPM-beveiligingschip 30
 - verificatie met Smart Card 47

J

- Java Card Security for HP ProtectTools
 - aanmaken, beheerder 40
 - beheerderstaken 39
 - Credential Manager 15
 - geavanceerde taken 39
 - gebruiker, aanmaken 41
 - lezer, selecteren 38

- opstartverificatie, inschakelen 40
 - opstartverificatie, instellen 40
 - opstartverificatie, uitschakelen 41
 - pincode 8
 - pincode, toewijzen 39
 - pincode, wijzigen 38
 - toewijzen, naam 39
- N**
- Netwerkkaccount 19
 - Noodherstel 30
- O**
- Ongeoorloofde toegang, voorkomen 6
 - Opstartopties 44
 - Opstartverificatie
 - bij opnieuw opstarten van Windows 50
 - in- en uitschakelen 47
 - Opstartwachtwoord
 - definitie 8
 - instellen en wijzigen 49
- P**
- Personal Secure Drive (PSD) 32
 - Problemen oplossen
 - Credential Manager 66
 - Device Access Manager 76
 - Embedded Security 69
 - overige problemen 77
- R**
- Registreren
 - applicatie 20
 - referenties 15
- S**
- Schijf decoderen 59
 - Security Setup (Beveiligingsinstellingen), wachtwoord 8
 - Single Sign On
 - applicaties exporteren 21
 - applicaties verwijderen 21
 - automatische registratie 20
 - eigenschappen van applicaties wijzigen 21
 - handmatige registratie 21
- Streng beveiliging 50
- T**
- Toegang
 - beheren 53
 - ongeoorloofde voorkomen 6
 - Toegang, HP ProtectTools Security 4
 - Token, Credential Manager 15
 - Token voor noodherstel, wachtwoord
 - definitie 8
 - instellen 30
 - TPM-beveiligingschip
 - initialiseren 30
 - inschakelen 30
- U**
- Uitschakelen
 - apparaatopties 44
 - Automatic DriveLock 48
 - Embedded Security 34
 - Embedded Security, blijvend 35
 - Java Card, opstartverificatie 41
 - opstartverificatie 47
 - streng beveiliging 50
 - verificatie met Smart Card 47
 - USB eToken, Credential Manager 16
- V**
- Vergrendelen, computer 18
 - Vingerafdrukken, Credential Manager 15
 - Virtueel token 17
 - Virtueel token, Credential Manager 15, 17
 - Voorzieningen, HP ProtectTools 2
- W**
- Wachtwoord
 - Basic User Key 33
 - beheren 7
 - beleid, definiëren 6
 - beveiligd, instellen 9
 - Computer Setup, beheren 48
 - eigenaar 30
 - herstellen, gebruiker 34
 - HP ProtectTools 7
 - instellen, instelwachtwoord 49
 - instellen, opstarten 49
 - instellen, opties 50
 - noodherstel, token 30
 - richtlijnen 9
 - wijzigen, eigenaar 34
 - wijzigen, instelwachtwoord 50
 - wijzigen, opstarten 49
 - Windows, aanmelden 17
 - Windows, aanmelden
 - Credential Manager 19
 - wachtwoord 8
 - Windows-netwerkkaccount 19

