HP ProtectTools
Felhasználói útmutató

Első kiadás: 2009. november

A dokumentum cikkszáma: 593308-211

Tartalomjegyzék

1 Bevezetés a biztonság világába

A HP ProtectTools Security Manager szoftver olyan biztonsági szolgáltatásokat nyújt, amelyekkel a számítógépek, a hálózatok és a fontos adatok megvédhetők az illetéktelen hozzáféréssel szemben. A HP ProtectTools Security Manager szoftvert az Administrative Console funkción keresztül lehet felügyelni.

A HP ProtectTools HP ProtectTools Administrative Console segítségével a rendszergazda az alábbi feladatokat tudja ellátni:

- Biztonsági funkciók engedélyezése és letiltása
- A számítógépet használók ujjlenyomatainak rögzítése
- Egy vagy több kép felvétele az arcfelismeréshez
- Intelligens kártya beállítása a hitelesítéshez
- Hitelesítő adatok megadása a hitelesítéshez
- A számítógép-felhasználók kezelése
- Az eszközspecifikus paraméterek beállítása
- A Security Manager telepített alkalmazásainak beállítása
- További Security Manager-alkalmazások hozzáadása

A Security Manager kezelőpaneljének segítségével az egyszerű felhasználók az alábbi feladatokat hajthatják végre:

- A rendszergazdák által elérhetővé tett beállítások konfigurálása
- Néhány HP ProtectTools-modul korlátozott felügyelete

A számítógéphez választható szoftvermodulok a számítógéptípustól függően változhatnak.

A HP ProtectTools szoftvermodulok előre telepítettek, előre betöltöttek, illetve a HP webhelyéről letölthetők lehetnek. További információért keresse fel a HP webhelyét: http://www.hp.com.

MEGJEGYZÉS: A jelen útmutatóban szereplő utasítások azon a feltételezésen alapulnak, hogy már sor került a megfelelő HP ProtectTools szoftvermodulok telepítésére.

A HP ProtectTools szolgáltatásai

Az alábbi táblázat tartalmazza a HP ProtectTools modulok legfontosabb funkcióit.

Modul	Fő szolgáltatások
HP ProtectTools Security Manager Administrative Console (rendszergazdáknak)	• A Security Manager telepítő varázsló segítségével megadhatja és beállíthatja a biztonsági szinteket és a biztonsági bejelentkezési eljárásokat. • A konfigurálási lehetőségeket az egyszerű felhasználók nem láthatják. • A Device Access Manager alkalmazás beállításainak és a felhasználói hozzáférés konfigurálása. • HP ProtectTools-felhasználók hozzáadása és eltávolítása, illetve a felhasználók státuszának megtekintése a rendszergazdai eszköz segítségével.
HP ProtectTools Security Manager (egyszerű felhasználóknak)	• A felhasználónevek és jelszavak rendezése, beállítása és módosítása. • A felhasználó hitelesítő adatainak – mint amilyen pl. a Windows-jelszó vagy a Smart Card – beállítása és módosítása. • A File Sanitizer (Fájlürítő) alkalmazás Shred (Szétfoszlatás), Bleaching (Kifehérítés) és Settings (Beállítások) funkcióinak konfigurálása és módosítása. • A Device Access Manager alkalmazás beállításainak megtekintése. • A Tulajdonságok, illetve a Biztonsági mentés és visszaállítás opcióinak konfigurálása.
Credential Manager for HP ProtectTools (Password Manager)	• A felhasználónevek és jelszavak elmentése, rendezése és védelme. • Webhelyek és programok kezdőképernyőinek beállítása a gyors és biztonságos elérés érdekében. • A biztonságos webhelyeken használt felhasználónevek és jelszavak elmentése a Password Managerrel. Ha a legközelebb meglátogatja ezt a webhelyet, a Password Manager automatikusan beírja és elküldi az adatokat. • Erősebb jelszavak létrehozása a felhasználói adatok fokozott biztonsága érdekében. A Password Manager automatikusan beírja és elküldi az adatokat.
Drive Encryption for HP ProtectTools (csak egyes típusokon)	• Teljes, mindenre kiterjedő merevlemez-titkosítás. • A rendszerindítási hitelesítés kikényszerítése az adatok megfejtéséhez és eléréséhez.
Privacy Manager for HP ProtectTools (csak egyes típusokon)	• Speciális belépési eljárások a kommunikáció forrásának, épségének és biztonságának ellenőrzésére e-mailezés, Microsoft® Office dokumentumok vagy azonnali üzenetküldő alkalmazások használata közben.

Modul	Fő szolgáltatások
File Sanitizer for HP ProtectTools	• A számítógépen található digitális erőforrások (a többek között alkalmazásfájlokból, előzményekből, internetes tartalmakból és egyéb bizalmas adatokból álló bizalmas információk) biztonságos szétfoszlatása, és a merevlemez rendszeres fehérítése.
Device Access Manager for HP ProtectTools (csak egyes típusokon)	• Az informatikai vezetők hozzáférés-kezelésének engedélyezése a felhasználói profilokon alapuló eszközökhöz. • Az illetéktelen felhasználók megakadályozása az adatok külső adattárolókkal történő eltávolításában és a rendszer külső médiaeszközökkel történő megfertőzésében. • Egyes felhasználók vagy felhasználói csoportok írható eszközökhöz való hozzáférésének rendszergazdai letiltása.

A fontosabb biztonsági feladatok

A HP ProtectTools program moduljai egymással együttműködve számos biztonsági problémára megoldást nyújtanak. Ezek többek között a következők:

- Védelem a célirányos lopással szemben
- Az érzékeny adatok elérésének korlátozása
- A külső és belső helyekről történő illetéktelen hozzáférés megakadályozása
- Erős jelszóvédelmi rend kialakítása

Védekezés a célirányos lopással szemben

A célirányos lopás egyik esete például egy bizalmas és ügyféladatokat tartalmazó számítógép ellopása egy repülőtéri ellenőrző pontról. Az alábbi funkciók segítik a célirányos lopással szembeni védekezést:

- A rendszerindítás előtti hitelesítés, amennyiben engedélyezve van, megakadályozza az operációs rendszer elérését. Lásd az alábbi műveleteket:
  - Security Manager
  - Drive Encryption

Az érzékeny adatok elérésének korlátozása

Tegyük fel, hogy a helyszínen egy kihelyezett könyvvizsgáló dolgozik, aki számítógépes hozzáféréssel rendelkezik a bizalmas pénzügyi adatok megtekintéséhez. Ön minden bizonnyal nem szeretné, ha a könyvvizsgáló ki tudná nyomtatni vagy írható adathordozóra, pl. CD-lemezre tudná írni a fájlokat. Az alábbi funkció korlátozza az érzékeny adatok elérését:

- A Device Access Manager for HP ProtectTools alkalmazás segítségével az informatikai vezetők korlátozni tudják az írható eszközökhöz való hozzáférést, így a bizalmas adatokat nem lehet a merevlemezről kinyomtatni, illetve cserélhető adathordozóra másolni.

A külső és belső helyekről történő illetéktelen hozzáférés megakadályozása

A nem titkosított üzleti személyi számítógépek illetéktelen elérése nagyon is kézzelfogható kockázatot jelent a vállalati hálózati erőforrásokra nézve, például információk pénzügyi szolgáltatásokról, egy igazgatóról, vagy kutatás-fejlesztési csoportról szóló, vagy olyan magánjellegű információk esetén, mint például betegadatok vagy személyes pénzügyi nyilvántartások. A következő szolgáltatások hozzájárulnak az illetéktelen hozzáférés megakadályozásához:

- A rendszerindítás előtti hitelesítés, amennyiben engedélyezve van, megakadályozza az operációs rendszer elérését. Lásd az alábbi műveleteket:
  - Password Manager
  - Drive Encryption
- A Password Manager alkalmazás biztosítja, hogy az illetéktelen felhasználók ne ismerjék meg a jelszavakat, és ne férjenek hozzá a jelszóval védett alkalmazásokhoz.

- A Device Access Manager for HP ProtectTools alkalmazás segítségével az informatikai vezetők korlátozni tudják az írható eszközökhöz való hozzáférést, így a bizalmas adatokat nem lehet a merevlemezről átmásolni.
- A File Sanitizer (Fájlürítő) alkalmazás lehetővé teszi az adatok biztonságos törlését, mivel szétfoszlatja a kritikus fájlokat és mappákat, illetve kifehéríti a merevlemezt (felülírva a már törölt, de még helyreállítható adatokat).
- A DriveLock biztosítja, hogy az adatokhoz akkor se lehessen hozzáférni, ha a merevlemezt eltávolították, és egy nem megbízható rendszerbe helyezték át.

Erős jelszóvédelmi rend kialakítása

Ha egy, több tucatnyi webalapú alkalmazás és adatbázis erős jelszóvédelmi renddel történő használatát megkívánó utasítás lépne érvénybe, a Security Manager védett jelszó-tárhelyet és az Egyszeri bejelentkezés alkalmazással járó kényelmet is biztosítja.

További biztonsági összetevők

A biztonsági szerepek kiosztása

A számítógép biztonságának kezelésében (különösen nagy vállalatok esetén) fontos gyakorlat a felelősségek és jogosultságok megosztása a különféle rendszergazdai és felhasználói típusok között.

MEGJEGYZÉS: Kisvállalati vagy egyéni felhasználás esetén ezek a szerepek ugyanarra a személyre is hárulhatnak.

A HP ProtectTools esetén a biztonsági kötelezettségek és jogosultságok a következő szerepekre oszthatók fel:

- Biztonsági felügyelő – meghatározza a vállalat vagy a hálózat biztonsági szintjét, és meghatározza a felépítés biztonsági jellemzőit (Java™-kártyák, biometrikus adatolvasók vagy USB-tokenek).

  MEGJEGYZÉS: A biztonságért felelős munkatárs a HP-val együttműködve a HP ProtectTools sok szolgáltatását testre szabhatja. További információkért lásd a HP webhelyét: http://www.hp.com.

- Rendszergazda – Alkalmazza és kezeli a biztonsági felügyelő által meghatározott biztonsági jellemzőket. Engedélyezhet és letilthat bizonyos szolgáltatásokat is. Például ha a biztonsági felügyelő úgy dönt, hogy Java-kártyákat használ, az IT-rendszergazda engedélyezheti a BIOS-biztonság Java-kártyás üzemmódját.

- Felhasználó – használja a biztonsági funkciókat. Például ha a biztonsági felügyelő és az IT-rendszergazda engedélyezte a Java-kártyák használatát a rendszerben, a felhasználó beállíthatja a kártya PIN-kódját, és a kártyát hitelesítésre használhatja.

VIGYÁZAT! A rendszergazdák a legmegfelelőbb gyakorlatnak megfelelően dönthetnek a végfelhasználói jogosultságok, illetve a hozzáférések korlátozásáról.

Az illetéktelen felhasználók nem kaphatnak rendszergazdai jogosultságot.

A HP ProtectTools-jelszavak kezelése

A HP ProtectTools Security Manager legtöbb szolgáltatása jelszóval védett. Az alábbi táblázat az általánosan használt jelszavakat, a jelszó beállításához használható szoftvermodult és a jelszó funkcióját sorolja fel.

Az IT-rendszergazda által beállított és használt jelszavakra ez a táblázat csak utalást tesz. Minden más jelszót általános felhasználók vagy rendszergazdák állíthatnak be.

HP ProtectTools-jelszó	Beállítva az alábbi modulban	Funkció
Windows-bejelentkezési jelszó	Windows® vezérlőpult vagy HP ProtectTools Security Manager	A manuális bejelentkezéshez és a különböző Security Manager funkciókhoz való hozzáférés hitelesítéséhez használható.
Security Manager Biztonsági mentés és helyreállítás jelszó	Security Manager, egyéni felhasználónként	Védi a Security Manager Biztonsági mentés és helyreállítási fájljához való hozzáférést.
A Java™-kártya PIN-kódja	Java Card Security	Védi a hozzáférést a Java-kártya tartalmához, és hitelesíti a Java-kártya felhasználóit. Bekapcsolási hitelesítéshez használva a Java-kártya PIN-kódja

HP ProtectTools-jelszó	Beállítva az alábbi modulban	Funkció
		korlátozza a hozzáférést a Computer Setup segédprogramhoz és a számítógép tartalmához is. Hitelesíti a Drive Encryption felhasználóit, ha a Java-kártya token ki van választva.

Biztonságos jelszó létrehozása

Jelszavak létrehozásakor elsősorban a program által megadott specifikációkat kell követni. Általában ajánlatos azonban a következő elveket figyelembe venni, amelyek segítségével erős jelszavak hozhatók létre, és így csökken az esély azok feltörésére:

- Legalább 6 karakterből, de inkább 8 karakterből álló jelszavakat használjon.
- Használjon vegyesen kis- és nagybetűket a jelszóban.
- Ha lehet, vegyesen használjon betűket és számokat, és alkalmazzon speciális karaktereket és írásjeleket.
- A jelszó egyes betűit helyettesítse speciális karakterekkel vagy számokkal. Használhatja például az 1-es számot az I vagy az L betű helyett.
- Kombináljon két vagy több nyelvből származó szavakat.
- Ossza fel a szót számokkal vagy speciális karakterekkel, például „Mary2-2Cat45”.
- Ne használjon olyan jelszót, amely megtalálható a szótárban.
- Ne használjon nevet vagy más személyes adatot, például születési dátumot, egy háziállat nevét vagy az anyja leánykori nevét jelszóként, még visszafelé írva sem.
- Rendszeresen módosítsa a jelszót. Elég lehet csak néhány karaktert megváltoztatni.
- Ha feljegyzi a jelszót, ne tárolja mások által is észrevehető helyen a számítógép közelében.
- Ne mentse fájlba, például egy e-mailbe a jelszót a számítógépen.
- Ne ossza meg másokkal a fiókokat, és ne árulja el a jelszavát senkinek.

A HP ProtectTools alkalmazásban lévő hitelesítési adatok biztonsági mentése és visszaállítása

A HP ProtectTools Biztonsági mentés és visszaállítás funkcióját a HP ProtectTools hitelesítési adatainak és beállításainak kijelöléséhez és biztonsági mentéséhez is használhatja.

2 A telepítő varázsló bemutatása

A HP ProtectTools telepítő varázsló végigvezeti Önt a Security Manager alkalmazás leggyakrabban használt funkcióinak telepítési folyamatán. A ProtectTools Administrative Console alkalmazáson keresztül ezenfelül még számos kiegészítő funkció is rendelkezésre áll. A varázslóban található beállításokat, illetve a kiegészítő biztonsági funkciókat a konzolból is elérheti és beállíthatja. A konzolt a Windows® Start menüjéből lehet megnyitni. A beállítások a számítógép teljes tartalmára és minden felhasználójára vonatkoznak.

1. Egy héttel a számítógép első telepítése után, bejelentkezéskor, vagy mikor egy rendszergazdai jogosultsággal rendelkező felhasználó először olvassa be az ujjlenyomatát, a Security Manager telepítő varázslója automatikusan elindul, és végigvezeti a program konfigurálásának legfontosabb lépésein. Automatikusan elindul a számítógép üzembe helyezését bemutató videó.

   – vagy –

   A HP ProtectTools Security Manager alkalmazást a Windows oldalsáv **Minialkalmazás** ikonjára vagy az értesítési területen, a tálca jobb szélén található ikonra kattintva tudja megnyitni.

   

   A Minialkalmazás ikon felső sávjának színe az alábbi állapotokat jelöli:

   - Piros: a HP ProtectTools még nincs beállítva, vagy hiba lépett fel a HP ProtectTools valamelyik moduljában.
   - Sárga: beállításmódosításokra van szükség. Ehhez tekintse meg a Security Manager alkalmazás Applications Status (Alkalmazások állapota) oldalát.
   - Kék: a HP ProtectTools beállítása kész, a működése pedig megfelelő.

   MEGJEGYZÉS: A Minialkalmazás ikon Windows XP operációs rendszerben nem áll rendelkezésre.

   – vagy –

Kattintson a **Start**, a **Minden program**, majd a **HP ProtectTools Administrative Console** lehetőségre.

2. Olvassa el az üdvözlőképernyőt, majd kattintson a **Tovább** gombra.

MEGJEGYZÉS: Az üdvözlőképernyőn kikapcsolhatja a varázsló további megjelenítését, ha a menüpontok valamelyikére kattint.

3. A telepítő varázsló felszólítja, hogy azonosítsa magát.

   Adja meg a Windows-jelszavát, vagy olvassa be az ujjlenyomatát az ujjlenyomat-olvasó segítségével, majd kattintson a **Next** (Tovább) gombra.

   Ha sem ujjlenyomat-olvasó, sem intelligens kártya nem áll rendelkezésre, a rendszer felszólítja, hogy adja meg a Windows-jelszavát. Ha bármikor hitelesítésre van szükség, ezt a jelszót kell megadnia.

   Ha még nem hozott létre Windows-jelszót, a rendszer felszólítja rá. A Windows-jelszóra azért van szükség, hogy megóvja a Windows felhasználói fiókot az illetéktelen hozzáféréstől, valamint, hogy Ön használni tudja a HP ProtectTools Security Manager alkalmazás funkcióit.

4. A telepítő varázsló végigvezeti a számítógép minden felhasználójára érvényes biztonsági funkciók telepítési folyamatán:

   - A Windows Logon Security alkalmazás biztosítja a Windows fiókok védelmét, mivel a felhasználóktól adott hitelesítési adatokat kíván meg a belépéshez.
   - A Drive Encryption alkalmazás a merevlemezek titkosításával védi meg az adatokat, mivel az engedély nélküli felhasználók nem nem tudják őket elolvasni.
   - A Pre-Boot Security alkalmazás még a Windows elindulása előtt megakadályozza az illetéktelen személyek hozzáférését az adatokhoz, így védi a számítógépet.

     MEGJEGYZÉS: A Pre-Boot Security alkalmazás nem áll rendelkezésre, ha a számítógépen lévő BIOS nem támogatja.

   Egy-egy biztonsági funkció engedélyezéséhez jelölje be a megfelelő négyzetet. Minél több funkciót engedélyez, annál biztonságosabb lesz a számítógép használata.

5. Kattintson a **Befejezés** gombra a varázsló zárólapján.

   Megjelenik a Security Manager kezelőpanelje.

MEGJEGYZÉS: Ha a varázslót korábban zárta be, az a későbbiekben még kétszer indul el automatikusan. Ezt követően a telepítés befejezéséig elérheti a varázslót a tálca jobb oldalán lévő értesítési területen megjelenő értesítési buborékban (hacsak ki nem kapcsolta).

3 HP ProtectTools Security Manager Administrative Console

A HP ProtectTools Security Manager szoftvert az Administrative Console alkalmazáson keresztül lehet felügyelni.

MEGJEGYZÉS: A HP ProtectTools alkalmazást csak rendszergazdai jogosultságokkal lehet felügyelni.

A konzollal az alábbi funkciókat lehet végrehajtani:

- Biztonsági funkciók engedélyezése és letiltása
- A számítógép-felhasználók kezelése
- Az eszközspecifikus paraméterek beállítása
- A Security Manager alkalmazásainak beállítása
- További Security Manager-alkalmazások hozzáadása

▲ A HP ProtectTools Security Managerben lévő alkalmazások használatához nyissa meg a HP ProtectTools Security Managert a Start menüben, vagy a jobb egérgombbal kattintson a Security Manager ikonra az értesítési területen, a tálca jobb szélén.

A HP ProtectTools Administrative Console és a benne lévő alkalmazások a számítógép valamennyi felhasználójának rendelkezésére állnak.

Az Administrative Console megnyitása

Rendszergazdai feladatok ellátásához, pl. a rendszer házirendjének megadásához vagy szoftverkonfiguráláshoz így nyissa meg a konzolt:

- Kattintson a **Start**, a **Minden program**, a **HP**, majd a **HP ProtectTools Administrative Console** elemre.

  – vagy –

  A Security Manager kezelőpaneljének bal oldali ablaktábláján kattintson az **Administration** (Felügyelet) elemre.

Felhasználói feladatok ellátásához, pl. ujjlenyomat-regisztráláshoz vagy a Security Manager alkalmazás futtatásához így nyissa meg a konzolt:

- Kattintson a **Start**, a **Minden program**, a **HP**, majd a **HP ProtectTools Security Manager** lehetőségre.

  – vagy –

  Kattintson duplán a tálca jobb szélén található értesítési területen a **HP ProtectTools Security Manager** ikonra.

Az Administrative Console használata

A Security Manager Administrative Console a HP ProtectTools Security Manager központi felügyeleti helye.

A konzol az alábbi részegységekből áll:

- **Eszközök**: az alábbi kategóriákat jeleníti meg a számítógép biztonságának konfigurálásához:
  - **Kezdőlap**: lehetővé teszi a szükséges biztonsági teendők végrehajtását.
  - **Rendszer**: lehetővé teszi a biztonsági funkciók beállítását, valamint a felhasználók és eszközök hitelesítését.
  - **Alkalmazások**: megjeleníti a HP ProtectTools Security Manager és a Security Manager alkalmazásaihoz tartozó általános beállításokat.
  - **Adatok**: megjelenít egy lenyitható menüt, amely a gépen lévő adatokat védő Security Manager-alkalmazásokra mutató hivatkozásokat tartalmaz.
- **Management Tools**: információt nyújt a további eszközökről. A panelen a következő választási lehetőségek jelennek meg:
  - **HP ProtectTools Security Manager telepítő varázsló**: végigvezeti a HP ProtectTools Security Manager telepítésén.
  - **Súgó**: megjeleníti a súgó fájlt, ami információt nyújt a Security Manager szoftverről és annak előre telepített alkalmazásairól. Az Ön által telepített újabb alkalmazások súgói az adott alkalmazásban találhatók.
  - **Névjegy**: megjeleníti a HP ProtectTools Security Manager adatait, pl. a verziószámot vagy a szerzői jogi információt.
- **Fő felület**: megjeleníti az egyes alkalmazásokhoz tartozó képernyőket.

4 A rendszer konfigurálása

A Rendszer csoportot a HP ProtectTools Administrative Console képernyőjének bal oldalán található Eszközök menüből lehet megnyitni. A csoportban található alkalmazások segítségével Ön a számítógéphez tartozó házirendet és beállításokat, illetve felhasználókat és eszközöket is felügyelheti.

A Rendszer csoport az alábbi alkalmazásokat tartalmazza:

- **Biztonság**: felügyeli a funkciókat, a hitelesítéseket, illetve a felhasználók számítógéppel történő kommunikációját irányító beállításokat.
- **Felhasználók**: megadja, felügyeli és regisztrálja a számítógép felhasználóit.
- **Eszközök**: felügyeli a számítógépbe épített vagy hozzá csatlakoztatott biztonsági eszközök beállításait.

A számítógéphez tartozó hitelesítések beállítása

A Hitelesítés alkalmazáson belül Ön kiválaszthatja, hogy mely biztonsági funkciók fussanak a számítógépen, beállíthatja a számítógéphez való hozzáférést szabályozó házirendeket, és további speciális beállításokat adhat meg. Megadhatja az egyes felhasználói osztályok hitelesítéséhez szükséges hitelesítési adatokat, amelyekre a Windowsba vagy az internetre, illetve a különböző programokba való bejelentkezéskor van szükség az egyes munkamenetek során.

A számítógéphez tartozó hitelesítések beállítása:

1. A Biztonság menüben kattintson a **Hitelesítés** elemre.
2. A bejelentkezési hitelesítés beállításához kattintson a **Bejelentkezési szabályok** lapra, végezze el a kívánt módosításokat, majd kattintson az **Alkalmaz** parancsra.
3. A munkamenet-hitelesítés beállításához kattintson a **Munkamenet-szabályok** lapra, végezze el a kívánt módosításokat, majd kattintson az **Alkalmaz** parancsra.

Bejelentkezési szabályok

A Windowsba bejelentkező felhasználók hitelesítéséhez szükséges hitelesítési adatokat felügyelő házirend meghatározása:

1. Az Eszközök menüben kattintson a **Biztonság**, majd a **Hitelesítés** pontra.
2. Kattintson egy felhasználói kategóriára a **Bejelentkezési szabályok** lapon.
3. Adja meg a kiválasztott felhasználói kategóriához szükséges hitelesítési adato(ka)t. Legalább egy hitelesítési adatot meg kell adnia.
4. Válassza ki, hogy a felhasználók hitelesítéséhez van-e szükség hitelesítési adatra (csak egyre), vagy, hogy az összes felsorolt hitelesítési adatot meg kell-e adni. Azt is beállíthatja, hogy a számítógéphez senki se tudjon hozzáférni.
5. Kattintson az **Alkalmaz** elemre.

Munkamenet-szabályok

A Windows munkamenetek során a HP ProtectToolsban lévő alkalmazásokhoz való hozzáféréshez szükséges hitelesítési adatokat felügyelő házirend meghatározása:

1. Az Eszközök menüben kattintson a **Biztonság**, majd a **Hitelesítés** pontra.
2. Kattintson egy felhasználói kategóriára a **Munkamenet-szabályok** lapon.
3. Adja meg a kiválasztott felhasználói kategóriához szükséges hitelesítési adato(ka)t.
4. Válassza ki, hogy a felhasználók hitelesítéséhez van-e szükség hitelesítési adatra (csak EGYRE), vagy, hogy az ÖSSZES felsorolt hitelesítési adatot meg kell-e adni. A HP ProtectTools szoftverhez hitelesítés nélkül is hozzáférhet.
5. Kattintson az **Alkalmaz** elemre.

Beállítások

Az alábbi biztonsági beállításokat engedélyezheti:

- **Az egylépéses bejelentkezés engedélyezése**: lehetővé teszi a Windows-bejelentkezés kihagyását a számítógép felhasználói számára, amennyiben a hitelesítésre a BIOS-ban vagy titkosított meghajtón került sor.
- **A HP SpareKey-hitelesítés engedélyezése a Windows-bejelentkezéshez**: lehetővé teszi a HP SpareKey funkció használatát a Windows-bejelentkezéshez a számítógép felhasználói számára, akkor is, ha a Security Manager további hitelesítési szabályokat kíván meg.

A beállítások szerkesztése:

1. Egy adott beállítás engedélyezéséhez vagy letiltásához kattintson a beállításra.
2. A módosítások mentéséhez kattintson az **Alkalmaz** lehetőségre.

A felhasználók kezelése

A Felhasználók alkalmazáson belül figyelemmel követheti és kezelheti a számítógépen található HP ProtectTools alkalmazás felhasználóit.

A HP ProtectTools valamennyi felhasználója fel van sorolva, és a rendszer ellenőrzi őket a Security Manager alkalmazásban beállított házirend szerint az alapján, hogy rendelkeznek-e a házirend követelményeinek megfelelő hitelesítési adatokkal, vagy sem.

A felhasználók kezeléséhez válasszon az alábbi beállítások közül:

- További felhasználók hozzáadásához kattintson a **Hozzáadás** elemre.
- Ha törölni kíván egy felhasználót, kattintson rá, majd a **Törlés** gombra.
- Ujjlenyomatok rögzítéséhez vagy további hitelesítő adatok beállításához kattintson a felhasználóra, majd a **Rögzítés** gombra.
- Egy adott felhasználóhoz tartozó szabályok megtekintéséhez kattintson a felhasználóra, és tekintse meg az szabályokat az alsó ablakban.

Az eszközbeállítások megadása

Az Eszköz alkalmazáson belül megadhatja a HP ProtectTools Security Manager által felismert, a rendszerbe épített vagy ahhoz csatlakoztatott bármilyen biztonsági eszköz beállításait.

Ujjlenyomatok

Az Ujjlenyomatok oldalon három lap található: a Rögzítés, az Érzékenység és a Speciális.

Rögzítés

Itt adhatja meg a felhasználók által rögzítendő ujjlenyomatok legalacsonyabb és legmagasabb számát.

Emellett az ujjlenyomat-olvasóban tárolt valamennyi adatot törölheti.

△ **VIGYÁZAT!** Ha minden adatot eltávolít az ujjlenyomat-olvasóból, akkor a felhasználók, köztük a rendszergazda ujjlenyomat-adatai is törlődnek. Ha a bejelentkezési szabályok csak az ujjlenyomatok megadását kívánják meg, ezután egyetlen felhasználó sem tud bejelentkezni a számítógépre.

Érzékenység

Az ujjlenyomat-olvasó beolvasási érzékenységének beállításához használja a csúszkát.

Ha a rendszer egy ujjlenyomatot rendszeresen nem ismer fel, állítsa alacsonyabbra az érzékenységet. A magasabb beállítás megnöveli a beolvasott ujjlenyomatok változatai iránti érzékenységet, így megnő a téves elfogadások esélye. A Közepes-magas beállítás egyszerre nyújt biztonságot és kényelmet.

Speciális

Itt beállíthatja, hogy az ujjlenyomat-olvasó energiát takarítson meg, ha a számítógép akkumulátorról üzemel.

Intelligens kártya

Itt beállíthatja a számítógép automatikus zárolását, ha az intelligens kártyát eltávolítják. A számítógép zárolására azonban csak akkor kerül sor, ha az intelligens kártyát hitelesítési adatként használták a Windowsba történő bejelentkezés során. Egy, a Windowsba történő bejelentkezés során nem használt intelligens kártya eltávolítása nem eredményezi a számítógép zárolását.

▲ Jelölje be a négyzetet, hogy engedélyezze vagy letiltsa a számítógép zárolását az intelligens kártya eltávolításakor.

Arc

Beállíthatja az Arcfelismerés biztonsági szintjét, hogy egyensúlyba hozza a könnyű használatot és a számítógép biztonsági rései által jelentett nehézségeket.

1. Kattintson a **Start**, a **Minden program**, a **HP**, majd a **HP ProtectTools Administrative Console** elemre.
2. Kattintson az **Eszközök**, majd az **Arc** elemre.

3. A kényelmesebb használatot a csúszka balra, a pontosságot a csúszka jobbra húzásával biztosíthatja.

   - A **Kényelem** funkció még könnyebb hozzáférést biztosít a jelentéktelen esetekben. Kattintson a csúszkára, és húzza a **Kényelem** állás irányába.
   - Az **Egyensúly** a biztonság és a kezelhetőség közötti egyensúly megteremtéséhez vagy olyankor használható, ha kényes adatai vannak, illetve ha a számítógép olyan helyen található, ahol illetéktelen bejelentkezési kísérletek fordulhatnak elő. Kattintson a csúszkára, és húzza az **Egyensúly** állás irányába.
   - A **Pontosság** bonyolultabbá teszi a felhasználók belépését, ha a felvett képek vagy a jelenlegi fényviszonyok nem szokványosak, és kevésbé valószínű, hogy téves elfogadás történik. Kattintson a csúszkára, és húzza a **Pontosság** állás irányába.

   MEGJEGYZÉS: A biztonsági szint minden felhasználóra érvényes.

4. Kattintson az **Alkalmaz** elemre.

Speciális beállítások

1. Kattintson a **Start**, a **Minden program**, a **HP**, majd a **HP ProtectTools Administrative Console** elemre.
2. Kattintson az **Eszközök**, majd az **Arc** elemre.
3. Kattintson a **Speciális** elemre.

   - **Belépés a Windowsba felhasználónév nélkül.**
     - Jelölje be a jelölőnégyzetet, hogy engedélyezze a felhasználók felhasználónév nélküli belépését a Windowsba.
     - Törölje a jelölést, ha azt szeretné, hogy a rendszer felhasználónevet kérjen a belépéshez.
   - **A PIN-kód használatának érvényesítése az arcfelismeréses bejelentkezésnél**: jelölje be a jelölőnégyzetet, ha azt szeretné, hogy minden felhasználó PIN-kódot hozzon létre és használjon a belépéshez.
     - **A PIN-kód minimálisan megengedett hossza**: kattintson a felfelé nyílra, ha növelni, vagy a lefelé nyílra, ha csökkenteni szeretné PIN-kódhoz szükséges karakterek minimális számát.
     - **A PIN-kód maximálisan megengedett hossza**: kattintson a felfelé nyílra, ha növelni, vagy a lefelé nyílra, ha csökkenteni szeretné PIN-kódhoz szükséges karakterek maximális számát.
     - **A PIN-kód beírásának maximálisan engedélyezett száma**: kattintson a felfelé nyílra, ha növelni, vagy a lefelé nyílra, ha csökkenteni szeretné PIN-kód megadási próbálkozásainak maximális számát.
4. Kattintson az **OK** gombra.

5 Az alkalmazások konfigurálása

Az Alkalmazások csoportot a HP ProtectTools Administrative Console bal oldalán található Biztonsági alkalmazások menüből lehet megnyitni. A Beállítások pont segítségével testre szabhatja a készülékre telepített HP ProtectTools Security Manager-alkalmazások viselkedését.

Az alkalmazások beállításainak szerkesztése:

1. Az Eszközök menüben, az **Alkalmazások** csoportban kattintson a **Beállítások** lehetőségre.
2. Egy adott beállítás engedélyezéséhez vagy letiltásához kattintson a beállításra.
3. A módosítások mentéséhez kattintson az **Alkalmaz** lehetőségre.

Általános lap

Az Általános lapon az alábbi beállítások állnak rendelkezésre:

- **Ne indítsa el automatikusan a rendszergazdai telepítő varázslót**: ezt a lehetőséget akkor válassza, ha nem szeretné, hogy a varázsló a bejelentkezéskor automatikusan megnyíljon.
- **Ne indítsa el automatikusan az Első lépések felhasználói varázslót**: ezt a lehetőséget akkor válassza, ha nem szeretné, hogy a felhasználói beállítások a bejelentkezéskor automatikusan megnyíljanak.

Alkalmazások lap

Az itt látható beállítások módosulhatnak, ha a Security Manager új alkalmazásokkal bővül. Az alapértelmezés szerint megjelenő minimális beállítások a következők:

- **Az alkalmazás állapota**: lehetővé teszi az összes alkalmazás állapotának megjelenítését.
- **Password Manager**: valamennyi felhasználó számára engedélyezi a Password Manager alkalmazás használatát.
- **Privacy Manager**: valamennyi felhasználó számára engedélyezi a Privacy Manager alkalmazás használatát.
- **A Bővebben gomb engedélyezése**: valamennyi felhasználó számára lehetővé teszi, hogy a **[+] Bővebben** gombra kattintva új alkalmazásokkal bővítse a HP ProtectTools Security Managert.

Ha az összes alkalmazást gyári állapotba kívánja visszaállítani, kattintson az **Alapértékek visszaállítása** gombra.

6 Felügyeleti eszközök

Kiegészítő alkalmazások akkor állnak rendelkezésre, ha a Security Manager új felügyeleti eszközökkel bővül. A számítógép rendszergazdája a Beállítások alkalmazáson keresztül letilthatja ezt a funkciót.

További felügyeleti eszközök hozzáadásához kattintson a **[+] Felügyeleti eszközök** elemre.

Frissítések és üzenetek

Ha van elérhető internetkapcsolat, látogasson el a DigitalPersona webhelyre (http://www.digitalpersona.com/), ahol új alkalmazásokat kereshet, és menetrendet állíthat be az automatikus frissítésekhez.

1. Ha információt szeretne kérni az új alkalmazásokról és frissítésekről, jelölje be a **Keep me informed about new applications and updates** (Értesítést kérek az új alkalmazásokról és frissítésekről) melletti négyzetet.
2. Az automatikus frissítések menetrendjének beállításához adja meg a napok számát.
3. Frissítéseket a **Check Now** (Ellenőrzés) gombra kattintva kereshet.

7 HP ProtectTools Security Manager

A HP ProtectTools Security Manager használatával jelentősen megnő a számítógép biztonsága.

Használhatja a Security Managerrel előre betöltött alkalmazásokat, valamint az internetről azonnal letölthető kiegészítő alkalmazásokat is:

- A bejelentkezés és a jelszavak kezelése
- A Windows® operációs rendszerben használt jelszó egyszerű cseréje
- A programjellemzők beállítása
- Ujjlenyomatok használata a kiemelt biztonság és kényelem érdekében
- Egy vagy több kép rögzítése az arcfelismeréshez
- Intelligens kártya beállítása a hitelesítéshez
- A programadatok biztonsági mentése és visszaállítása
- További alkalmazások hozzáadása

A HP ProtectTools Security Manager megnyitása

A HP ProtectTools Security Managert az alábbi módszerek valamelyikével tudja megnyitni:

- Kattintson a **Start**, a **Minden program**, a **HP**, majd a **HP ProtectTools Security Manager** lehetőségre.
- A jobb egérgombbal kattintson az értesítési területen (a tálca jobb szélén) található **HP ProtectTools** ikonra.
- A jobb egérgombbal kattintson a **HP ProtectTools** ikonra, majd kattintson **A HP ProtectTools Security Manager megnyitása** parancsra.
- Kattintson a **Security Manager ID Card** (Security Manager azonosító kártyája) minialkalmazásra a Windows oldalsávon.
- A Security Manager gyorshivatkozás-menüjének megnyitásához nyomja le a ctrl+Windows+h gyorsbillentyű-kombinációt.

A Security Manager műszerfalának használata

A Security Manager kezelőpanelje a Security Managerben található funkciók, alkalmazások és beállítások központi hozzáférési helye.

▲ A Security Manager kezelőpaneljének megnyitásához kattintson a **Start**, a **Minden program**, a **HP**, majd a **HP ProtectTools Security Manager** lehetőségre.

A kezelőpanel az alábbi részegységekből áll:

- **Azonosító kártya**: megjeleníti a Windows-felhasználó nevét és egy kiválasztott képet, amely azonosítja a bejelentkezett felhasználói fiókot.
- **Biztonsági alkalmazások**: megjelenít egy lenyitható menüt, amely az alábbi biztonsági kategóriák beállítására mutató hivatkozásokat tartalmaz:
  - **Hitelesítési kezelőszoftver**
  - **Saját adatok**
- **Bővebben**: megnyit egy, a személyazonosság, az adatok és kapcsolatok biztonságát növelő kiegészítő alkalmazásokat tartalmazó oldalt.
- **Fő felület**: megjeleníti az egyes alkalmazásokhoz tartozó képernyőket.
- **Felügyelet**: megnyitja a HP ProtectTools Administrative Console-t.
- **Súgó gomb**: megjeleníti az aktuális képernyő adatait.
- **Speciális**: lehetővé teszi a következő opciók használatát:
  - **Tulajdonságok**: a segítségével testre szabhatja a Security Manager beállításait.
  - **Biztonsági mentés és visszaállítás**: lehetővé teszi az adatok biztonsági mentését és visszaállítását.
  - **Névjegy**: megjeleníti a Security Manager verzióadatait.

Beállítási eljárások

A hitelesítési adatok regisztrálása

A My Identity (Saját azonosító) oldalt a különféle hitelesítési eljárások vagy hitelesítési adatok regisztrálására használhatja. A regisztráció után ezeket az eljárásokat a Security Manager alkalmazásba való bejelentkezéshez használhatja.

Az ujjlenyomatok rögzítése

Ha a számítógép rendelkezik beépített vagy hozzá csatlakoztatott ujjlenyomat-olvasóval, a HP ProtectTools Security Manager telepítő varázslója végigvezeti az ujjlenyomatok beállításának vagy rögzítésének folyamatán.

1. Megjelenik két kéz körvonala. A már rögzített ujjlenyomatokhoz tartozó ujjak zöld színnel vannak kiemelve. Kattintson az egyik ujjra a kéz körvonalán.

   MEGJEGYZÉS: Ha törölni szeretne egy korábban rögzített ujjlenyomatot, kattintson a megfelelő ujjra.

2. Ha kiválasztotta a rögzíteni kívánt ujjat, a rendszer felkéri, hogy az ujját addig tartsa a leolvasón, amíg sikeresen rögzítésre nem kerül. A rögzített ujjlenyomathoz tartozó ujj zöld színnel van kiemelve a kéz körvonalán.

3. Legalább két ujjának lenyomatát rögzítenie kell; a mutató- és a középső ujj javasolt. Újabb ujjlenyomat rögzítéséhez ismételje meg az 1–3. lépést.

4. Kattintson a **Tovább** gombra, és kövesse a képernyőn megjelenő utasításokat.

MEGJEGYZÉS: Ha az ujjlenyomatát az Első lépések folyamat segítségével rögzítette, az ujjlenyomat-adatokat csak a **Tovább** gombra kattintással tudja elmenteni. Ha egy darabig nem használja a számítógépet, vagy ha bezárja a programot, a módosítások mentése **nem** történik meg.

Képek rögzítése

Az arcfelismeréshez egy vagy több képet kell rögzítenie.

Új kép rögzítése a HP ProtectTools Security Manager telepítő varázsló segítségével:

1. Kattintson a **HP ProtectTools Security Manager** ikonra a képernyő jobb oldalán lévő eszköztáron.

2. Írja be és hagyja jóvá a Windows® jelszavát, majd kattintson a **Tovább** gombra.

3. A **Biztonsági funkciók engedélyezése** menüben jelölje be a **Windows Logon Security** jelölőnégyzetet, majd kattintson a **Tovább** gombra.

4. A **Hitelesítési adatok kiválasztása** menüben jelölje be az **Arc** jelölőnégyzetet, majd kattintson a **Tovább** gombra.

5. Kattintson az **Enroll a new scene** (Új kép rögzítése) pontra.

A sikeres rögzítés után készíthet egy újabb képet, ha gondjai akadtak a bejelentkezés során, mert az alábbi feltételek közül egy vagy több megváltozott:

- Az arca az utolsó képrögzítés óta jelentősen megváltozott.
- A korábbi képekhez képest megváltoztak a fényviszonyok.
- A legutolsó felvételen szemüveget viselt (vagy nem viselt).

MEGJEGYZÉS: Ha a képek rögzítése során problémát tapasztal, vigye közelebb őket a webkamerához. A fényképekhez és videofelvételekhez hasonlóan a megvilágítás és a kontraszt rendkívül fontos. Ellenőrizze, hogy a munkamenethez kiválasztott megvilágítás elsősorban az előteret, ne pedig a hátteret világítsa meg. Ha úgy tapasztalja, hogy a Face Recognition arcfelismerő segédprogram nem képes Önt teljesen azonosítani, rögzítse újra a képet jobb megvilágítással.

Új kép rögzítése a HP ProtectTools Security Manager telepítő varázsló segítségével:

1. Kattintson a **Start**, a **Minden program**, a **HP**, majd a **HP ProtectTools Security Manager** lehetőségre.
2. Kattintson a **Hitelesítő adatok**, majd az **Arc** elemre.
3. Kattintson az **Enroll a new scene** (Új kép rögzítése) pontra.

Speciális felhasználói beállítások

1. Kattintson a **Start**, a **Minden program**, majd a **HP ProtectTools Security Manager** lehetőségre.
2. Kattintson a **Set up your authentication credentials** (Hitelesítő adatok beállítása), majd a **Face** (Arc) elemre.
3. Kattintson az **Advanced** (Speciális) gombra, majd válasszon a következő opciók közül.

   a. Ha PIN-kódos azonosítást szeretne az arcképes belépéshez, kattintson a **Create PIN** (PIN-kód létrehozása) parancsra, adja meg a Windows-jelszavát, írja be az új PIN-kódot, majd írja be ismét a jóváhagyáshoz.

   b. Ha kívánja, válasszon további beállításokat. Ezek a beállítások csak az aktuális felhasználóra érvényesek:

   - **Dallam lejátszása arcfelismeréskor**
     - Jelölje be a négyzetet, ha azt szeretné, hogy a számítógép a sikeres vagy hibás arcfelismerést dallammal jelezze.
     - Az opció kikapcsolásához törölje a jelölést a négyzetből.
   - **Képfrissítés, ha a belépés nem sikerül**
     - Jelölje be a jelölőnégyzetet, ha azt szeretné, hogy a felhasználó frissíthesse a képeit, ha az arcképes belépés nem sikerül. Ha az ellenőrzés eléri a „lehetséges” küszöbértéket, a felhasználónak el kell döntenie, hogy beilleszti-e a „hibás” belépés élő képeit a jelenlegi felvételbe, ezzel is növelve a későbbi sikeres belépések lehetőségét.
     - Az opció kikapcsolásához törölje a jelölést a négyzetből.
   - **Új kép készítése sikertelen belépés esetén**
     - Jelölje be a jelölőnégyzetet, hogy megjelenjen az ablak, amely a felhasználót arra kéri, hogy készítsen új képet, ha nem sikerül az arcképes belépés, és az ellenőrzés nem éri el a „lehetséges” küszöbértéket. Ez a következő alkalommal növelheti a sikeres belépés lehetőségét.
     - Az opció kikapcsolásához törölje a jelölést a négyzetből.

   c. Új kép rögzítéséhez kattintson az **Új kép rögzítése** pontra, majd kövesse a képernyőn megjelenő utasításokat.

A Windows-jelszó módosítása

A Security Manager segítségével a Windows-jelszó könnyebben és gyorsabban módosítható, mint a Windows Vezérlőpult használatával.

A Windows-jelszó módosításához tegye a következőket:

1. Kattintson a **Hitelesítési adatok** elemre, majd a **Jelszó** pontra a Security Manager kezelőpaneljén.
2. Adja meg az aktuális jelszót az **Aktuális Windows-jelszó** mezőben.

3. Írjon egy új jelszót az **Új Windows-jelszó** mezőbe, majd ismét írja be az **Új jelszó megerősítése** mezőbe.

4. Az aktuális jelszónak a most megadottra történő azonnali cseréjéhez kattintson a **Módosítás** lehetőségre.

Intelligens kártya beállítása

Az intelligens kártyás bejelentkezés kiválasztása után, ha a számítógép rendelkezik beépített vagy hozzá csatlakoztatott intelligenskártya-olvasóval, a Security Manager telepítő varázslója felkéri, hogy készítsen egy PIN-kódot (személyes azonosító szám) az intelligens kártyához.

Az intelligens kártya PIN-kódjának beállítása:

1. Adjon meg és hagyjon jóvá egy PIN-kódot az **Intelligens kártya beállítása** oldalon.

   A PIN-kódot módosítani is tudja. Írja be az aktuális PIN-kódot, majd adjon meg helyette egy újat.

2. A folytatáshoz kattintson a **Tovább** gombra, és kövesse a képernyőn megjelenő utasításokat.

– vagy –

▲ Kattintson a **Hitelesítési adatok** elemre, majd az **Intelligens kártya** pontra a Security Manager kezelőpaneljén.

- Az intelligens kártya PIN-kódjának beállítása: adjon meg és hagyjon jóvá egy PIN-kódot az **Intelligens kártya beállítása** oldalon.
- A PIN-kód módosítása: először adja meg a jelenlegi PIN-kódot, majd írja be és hagyja jóvá az újat.

Általános feladatok

Az ebbe a csoportba tartozó alkalmazások több szempontból is segítenek a digitális személyazonosság kezelésében.

- **Security Manager**: gyorshivatkozásokat hoz létre és kezel, amelyek segítségével webhelyeket és programokat nyithat meg úgy, hogy a Windows-jelszavával, az ujjlenyomatával vagy egy intelligens kártyával hitelesíti magát.
- **Hitelesítési adatok**: eszközként szolgál a Windows-jelszó egyszerű módosításához, az ujjlenyomatok rögzítéséhez, illetve az intelligenskártya-beállításhoz.

További alkalmazások hozzáadásához kattintson a műszerfal bal alsó sarkában található [+] **Bővebben** gombra. Lehetséges, hogy a rendszergazda letiltotta a gombot.

Password Manager

A Password Manager megkönnyíti és biztonságosabbá teszi a Windowsba, az internetre és az egyes alkalmazásokba történő bejelentkezést. Az alkalmazás segítségével erősebb jelszavakat hozhat létre, amelyeket nem kell fel- vagy megjegyeznie, majd az ujjlenyomata, az intelligens kártya vagy a Windows-jelszava segítségével gyorsan és könnyedén bejelentkezhet.

A Password Manager az alábbi lehetőségeket nyújtja:

- Bejelentkezések hozzáadása, szerkesztése vagy törlése a Kezelés lapon.
- Gyorshivatkozások használata az alapértelmezett böngésző megnyitásához, és ennek beállítása után bejelentkezés bármely webhelyre vagy programba.
- A gyorshivatkozások kategóriákba rendezése áthúzással.
- A jelszavak esetleges biztonsági kockázatának azonnali felmérése, és összetett, erős jelszavak automatikus létrehozása az új oldalakhoz.

A Password Manager számos funkciója a Password Manager ikonjára kattintva is elérhető, amely akkor látható, ha egy webhely vagy program bejelentkezési képernyője van középen. Kattintson az ikonra a helyi menü megjelenítéséhez, amelyből az alábbi menüpontok közül válogathat.

Olyan webhelyek vagy programok esetén, amelyekhez még nem készült bejelentkezés

A helyi menüben az alábbi menüpontok láthatók:

- **A [valamilyendomain.hu] hozzáadása a Password Managerhez**: a segítségével bejelentkezést adhat hozzá az aktuális bejelentkezési képernyőhöz.
- **A Password Manager megnyitása**: megnyitja a Password Managert.
- **Ikonbeállítások**: a segítségével megadhatja, hogy a Password Manager ikonja mikor jelenjen meg.
- **Súgó**: megjeleníti a Password Manager szoftversúgóját.

Olyan webhelyek vagy programok esetén, amelyekhez már készült bejelentkezés

A helyi menüben az alábbi menüpontok láthatók:

- **A bejelentkezési adatok kitöltése**: a bejelentkezési adatokat a bejelentkezési mezőkbe illeszti, majd elküldi az oldalra (ha a bejelentkezés létrehozása vagy legutóbbi szerkesztése során erre szükség volt).
- **A bejelentkezés szerkesztése**: a segítségével szerkesztheti az adott webhelyhez tartozó bejelentkezési adatait.
- **Új fiók hozzáadása**: a segítségével új fiókot adhat egy-egy bejelentkezéshez.
- **A Password Manager megnyitása**: megnyitja a Password Manager alkalmazást.
- **Súgó**: megjeleníti a Password Manager szoftversúgóját.

MEGJEGYZÉS: Lehetséges, hogy a számítógép rendszergazdája úgy állította be a Password Managert, hogy a személyazonossága igazolása során Önnek nemcsak egy hitelesítési adatot kell megadnia.

Bejelentkezések hozzáadása

A bejelentkezési adatok egyszeri megadásával Ön könnyen hozzáadhat egy bejelentkezést egy-egy webhelyhez vagy programhoz. A Password Manager onnantól automatikusan megadja ezeket az adatokat. A bejelentkezéseket a webhely vagy program megkeresése után használhatja, vagy kattintson egy bejelentkezésre a **Logons** (Bejelentkezések) menüben, ha szeretné, hogy a Password Manager megnyisson egy webhelyet vagy programot, és bejelentkezzen oda.

Bejelentkezés hozzáadása:

1. Nyissa meg a webhely vagy program bejelentkezési képernyőjét.
2. Kattintson a **Password Manager** ikonon található nyílra, majd kattintson az alábbiakra, attól függően, hogy a bejelentkezési képernyő egy webhelyhez vagy programhoz tartozik-e:
   - Webhelyek esetén kattintson **A [domainnév] hozzáadása a Password Managerhez** parancsra.
   - Programok esetén kattintson **A mostani bejelentkezési képernyő hozzáadása a Password Managerhez** parancsra.
3. Adja meg bejelentkezési adatait. A képernyő bejelentkezési mezőit, valamint a párbeszédablak megfelelő mezőit vastag, narancssárga keret jelzi. A párbeszédpanelt a **Password Manager kezelése** lapon található **Bejelentkezés hozzáadása** lehetőségre kattintva is megjelenítheti. Egyes lehetőségek a számítógéphez csatlakoztatott biztonsági eszközöktől függenek; ilyen pl. a ctrl+Windows+h gyorsbillentyűk használata, az ujjlenyomat beolvasása, illetve az intelligens kártyák behelyezése.
   a. Ha az egyik bejelentkezési mezőt az egyik előre formázott lehetőség segítségével kívánja kitölteni, kattintson a mező jobb oldalán lévő nyilakra.
   b. A bejelentkezéshez tartozó jelszót a **Jelszó megjelenítése** elemre kattintva tekintheti meg.
   c. Ha szeretné kitölteni a bejelentkezési mezőket, de a bejelentkezést nem kívánja elküldeni, törölje a jelölést a **Bejelentkezési adatok automatikus elküldése** melletti négyzetből.
   d. Kattintson az **OK** gombra, majd a használni kívánt hitelesítési eljárásra: **Ujjlenyomatok**, **Jelszó** vagy **Arc**, majd jelentkezzen be a kiválasztott hitelesítési eljárás segítségével.

Ha a Password Manager ikonja mellől hiányzik a pluszjel, az jelzi, hogy létrejött a bejelentkezés.

e. Ha a Password Manager nem észleli a bejelentkezési mezőket, kattintson a **Még több mező** gombra.

   i. Jelölje be a bejelentkezéshez szükséges jelölőnégyzeteket, vagy törölje azoknak a mezőknek a jelölését, amelyek nem szükségesek a bejelentkezéshez.

   ii. Ha a Password Manager nem észleli az összes bejelentkezési mezőt, egy megjelenő üzenet megkérdezi, hogy szeretné-e folytatni. Kattintson az **Igen** gombra.

   iii. Megjelenik egy párbeszédpanel a kitöltött bejelentkezési mezőkkel. Kattintson az egyes mezők ikonjára, és húzza át a megfelelő bejelentkezési mezőbe, majd kattintson a gombra, hogy belépjen a weboldalra.

   MEGJEGYZÉS: Mivel az oldal bejelentkezési adatainak beírásához a manuális módot használta, ha erre a weboldalra akar belépni, a jövőben is ezt a módszert kell használnia.

   MEGJEGYZÉS: A bejelentkezési adatokat manuális módszerrel csak az Internet Explorer 8-ban adhatja meg.

   iv. Kattintson a **Bezárás** gombra.

Valahányszor meglátogatja az adott webhelyet vagy megnyitja az adott programot, megjelenik a Password Manager ikonja is, amely így jelzi, hogy Ön a regisztrált hitelesítési adatokkal tud bejelentkezni.

Bejelentkezések szerkesztése

A bejelentkezések az alábbi lépésekkel szerkeszthetők:

1. Nyissa meg a webhely vagy program bejelentkezési képernyőjét.
2. Ha meg szeretne jeleníteni egy párbeszédpanelt, amelyben szerkesztheti a bejelentkezési adatait, kattintson a **Password Manager** ikonon található nyílra, majd a **Bejelentkezés szerkesztése** parancsra. A képernyőn látható bejelentkezési mezők és a párbeszédpanelen hozzájuk tartozó mezők vastag narancssárga kerettel vannak kiemelve.

   A párbeszédpanelt a **Password Manager kezelése** lapon található **Módosítás a kívánt bejelentkezésre** lehetőségre kattintva is megjelenítheti.
3. Szerkessze bejelentkezési adatait.
   - Egy bejelentkezési mezőnek egy előre formázott választás felhasználásával történő kitöltéséhez kattintson a mező jobb oldalán található nyilakra.
   - Ha a képernyőről további mezőket szeretne hozzáadni a bejelentkezéshez, kattintson a **Még több mező** elemre.
   - Ha szeretné kitölteni a bejelentkezési mezőket, de a bejelentkezést nem kívánja elküldeni, törölje a jelölést a **Bejelentkezési adatok elküldése** melletti négyzetből.
   - A bejelentkezéshez tartozó jelszót a **Jelszó megjelenítése** elemre kattintva tekintheti meg.
4. Kattintson az **OK** gombra.

A Logons (Bejelentkezések) menü használata

A Password Managerrel egyszerűen és gyorsan megnyithatja azokat a webhelyeket és programokat, amelyekhez bejelentkezést hozott létre. A bejelentkezési képernyő megnyitásához kattintson duplán egy programhoz vagy webhelyhez tartozó bejelentkezésre a **Bejelentkezések** menüben vagy a **Password Manager** alkalmazás **Bejelentkezések** lapján, majd adja meg a bejelentkezési adatokat.

Ha bejelentkezést hoz létre, az automatikusan a Password Manager alkalmazás Bejelentkezések menüjéhez adódik.

A Bejelentkezések menü megjelenítése:

1. Nyomja le a **Password Manager** alkalmazáshoz tartalmazó gyorsbillentyű-kombinációt, ami a gyári alapértelmezés szerint a ctrl+Windows+h. A gyorsbillentyű-kombináció módosításához kattintson a **Password Manager**, majd a **Settings** (Beállítások) lehetőségre.
2. Olvassa be az ujjlenyomatát (ha a számítógép rendelkezik beépített vagy hozzá csatlakozatott ujjlenyomat-olvasóval).

A bejelentkezések kategóriákba rendezése

A bejelentkezések rendszerezéséhez hozzon létre egy vagy több kategóriát. Ezután húzza az adott bejelentkezést a kívánt kategóriába.

Kategória hozzáadása:

1. Kattintson a **Password Manager** elemre a Security Manager műszerfalán.
2. Kattintson a **Kezelés** lapra, majd a **Kategória hozzáadása** elemre.
3. Adjon meg egy kategórianevet.
4. Kattintson az **OK** gombra.

Bejelentkezés hozzáadása egy-egy kategóriához:

1. Húzza a mutatót a kívánt bejelentkezés fölé.
2. Nyomja meg és tartsa lenyomva az egér bal gombját.
3. Húzza a bejelentkezést a kategórialistába. A kategóriák kiemelődnek, ha föléjük húzza az egeret.
4. A kívánt kategória kijelölt állapotában engedje el az egérgombot.

A bejelentkezések nem átkerülnek, hanem csak átmásolódnak a kiválasztott kategóriába. Ugyanazt a bejelentkezést több kategóriához is hozzáadhatja. Az összes bejelentkezést a **Mind** elemre kattintva jelenítheti meg.

A bejelentkezések kezelése

A Password Managerrel könnyen, egy központi helyről kezelheti a felhasználónevekhez, jelszavakhoz, illetve több bejelentkezési fiókhoz tartozó bejelentkezési adatokat.

A bejelentkezések a Manage (Kezelés) lapon vannak felsorolva. Ha ugyanahhoz a webhelyhez több bejelentkezést is létrehozott, a listán a webhely neve mellett, bekezdésekbe szedve az összes szerepel.

A bejelentkezések kezelése:

A Security Manager műszerfalán kattintson a **Password Manager** elemre, majd a **Kezelés** lapra.

- **Bejelentkezés hozzáadása**: kattintson a **Bejelentkezés hozzáadása** elemre, és kövesse a képernyőn megjelenő utasításokat.
- **Bejelentkezés szerkesztése**: kattintson az egyik bejelentkezésre, majd a **Szerkesztés** elemre, és módosítsa a bejelentkezési adatokat.
- **Bejelentkezés törlése**: kattintson az egyik bejelentkezésre, majd a **Törlés** elemre.

További bejelentkezés hozzáadása egy webhelyhez vagy programhoz:

1. Nyissa meg a webhely vagy program bejelentkezési képernyőjét.
2. A helyi menü megjelenítéséhez kattintson a **Password Manager** ikonra.
3. Kattintson az **Add additional logon** (További bejelentkezés hozzáadása) elemre, és kövesse a képernyőn megjelenő utasításokat.

A jelszó erősségének felmérése

A személyazonosság megvédésének fontos része, hogy a webhelyekre és programokba történő bejelentkezések során erős jelszót használjon.

A Password Manager a webhelyekre és programokba való bejelentkezések során használt jelszavak erősségének azonnali és automatikus elemzésével könnyedén nyomon követi és javítja a biztonságot.

A Password Manager ikon beállításai

A Password Manager megkísérli azonosítani a webhelyekhez és programokhoz tartozó bejelentkezési képernyőket. Ha olyan képernyőt észlel, amelyhez Ön még nem hozott létre bejelentkezést, a Password Manager felszólítja, hogy adjon meg egy bejelentkezést a képernyőhöz. Ehhez a Password Manager ikonja mellett egy + jel látható.

Kattintson az ikonon található nyílra, majd az **Ikonbeállítások** lehetőségre, hogy beállítsa, hogyan kezelje a **Password Manager** a lehetséges bejelentkezési oldalakat.

- **Szólítson fel bejelentkezések hozzáadására a bejelentkezési képernyőkhöz**: erre a lehetőségre akkor kattintson, ha szeretné, ha a Password Manager bejelentkezés hozzáadására szólítaná fel, ha olyan bejelentkezési képernyő jelenik meg, amelyhez még nincs beállítva egy.
- **A képernyő kihagyása**: a négyzet bejelölésével a Password Manager nem szólítja fel bejelentkezés hozzáadására ehhez a bejelentkezési képernyőhöz.

A Password Manager további beállításainak eléréséhez kattintson a **Password Manager**, majd a **Beállítások** lehetőségre a Security Manager műszerfalán.

Beállítások

A HP ProtectTools Security Managert különböző beállítások segítségével szabhatja testre:

1. **Szólítson fel bejelentkezések hozzáadására a bejelentkezési képernyőkhöz**: a Password Manager pluszjellel jelölt ikonja minden alkalommal megjelenik, amikor webhely vagy program bejelentkezési képernyőjét észleli. Ezzel jelzi, hogy az adott képernyőhöz történő bejelentkezés a jelszóvédőhöz adható. A funkció letiltásához vegye ki a **Szólítson fel bejelentkezések hozzáadására a bejelentkezési képernyőkhöz** elem melletti négyzetben lévő jelölést az **Ikonbeállítások** párbeszédpanelen.

2. **A Password Manager megnyitása a ctrl+Windows+h billentyűkombinációval**: a Password Manager gyorshivatkozások menüjét megnyitó alapértelmezett gyorsbillentyű-kombináció a ctrl +Windows+h. A gyorsbillentyű-kombináció módosításához kattintson erre a pontra, majd adjon meg egy új billentyűkombinációt. A kombinációk az alábbiak lehetnek: ctrl, alt vagy shift, illetve bármelyik betű- vagy számbillentyű.

3. A módosítások mentéséhez kattintson az **Alkalmaz** gombra.

Hitelesítési adatok

A Security Manager hitelesítési adatainak használata arra szolgál, hogy igazolja a felhasználó személyazonosságát. A számítógép rendszergazdája állítja be, hogy a Windows-fiókjába, webhelyekre vagy programokba történő bejelentkezések során mely hitelesítési adatokra van szükség a személyazonosság igazolásához.

A rendelkezésre álló hitelesítési adatok a számítógépbe épített vagy hozzá csatlakoztatott biztonsági eszközöktől függnek. Minden támogatott hitelesítési adattal be lehet lépni a **Saját azonosító, hitelesítési adatok** csoportba.

Fel vannak sorolva a rendelkezésre álló hitelesítési adatok, követelmények és az aktuális állapot, amelyek az alábbiak lehetnek:

- Ujjlenyomatok
- Jelszó
- Intelligens kártya
- Arc

Egy hitelesítési adat rögzítéséhez vagy módosításához kattintson a hivatkozásra, majd kövesse a képernyőn megjelenő utasításokat.

Személyi azonosító kártya

Az azonosító kártya a Windows-fiók kizárólagos tulajdonosaként azonosítja Önt, és megjeleníti a nevét és az Ön által választott képet. Az adatok kiemelve, a Windows oldalsávban lévő minialkalmazásként jelennek meg a Security Manager oldalainak bal felső sarkában.

A Windows oldalsávban található azonosító kártyára kattintva szintén gyorsan meg tudja nyitni a Security Manager alkalmazást.

Ön módosíthatja a képet és a nevének megjelenítési formáját. Alapértelmezés szerint a teljes Windows-beli név és a Windows telepítése során kiválasztott kép jelenik meg.

A megjelenített név módosítása:

1. Kattintson az **Azonosító kártya** ikonra a bal felső sarokban a Security Manager kezelőpaneljén.
2. Kattintson a Windows-fiók létrehozása során megadott név melletti jelölőnégyzetre. A rendszer ehhez a fiókhoz a Windows-beli felhasználónevet jeleníti meg.
3. A név módosításához adjon meg egy új nevet, majd kattintson a **Mentés** gombra.

A megjelenített kép módosítása:

1. Kattintson az **Azonosító kártya** elemre a bal felső sarokban a Security Manager kezelőpaneljén.
2. Kattintson a **Képválasztás** gombra, majd az egyik képre, végül pedig a **Mentés** gombra.

A beállítások megadása

Ön testre szabhatja a HP ProtectTools Security Manager beállításait. Kattintson a **Speciális**, majd a **Tulajdonságok** elemre a Security Manager műszerfalán. A rendelkezésre álló beállítások két lapon jelennek meg. Ezek a következők: Általános és Ujjlenyomat.

Általános

Az Általános lapon az alábbi beállítások állnak rendelkezésre:

Megjelenítés – ikon megjelenítése a tálcán

- Ha szeretné, hogy az ikon megjelenjen a tálcán, jelölje be a négyzetet.
- Ha nem szeretné, hogy az ikon megjelenjen a tálcán, vegye ki a négyzetből a jelölést.

Ujjlenyomat

Az Ujjlenyomat lapon az alábbi beállítások állnak rendelkezésre:

- **Gyorsműveletek**: a Gyorsműveletek funkcióval választhatja ki a végrehajtandó Security Manager-feladatot, amikor az ujjlenyomat-beolvasás közben lenyomva tartja a megfelelő billentyűt.

  A felsorolt billentyűk egyikéhez hozzárendelhet egy Gyorsműveletet, ha rákattint egy **(Billentyű) + Ujjlenyomat** opcióra, majd kiválaszt egy elérhető feladatot a menüből.

- **Visszajelzés a beolvasott ujjlenyomatról**: csak akkor látható, ha a rendszerben van ujjlenyomat-olvasó. Ezt a beállítást akkor használja, ha visszajelzést szeretne kérni az ujjlenyomat-beolvasás után.

  - **Hangvisszajelzés engedélyezése**: a Security Manager hangvisszajelzést ad, ha egy ujjlenyomat beolvasása kész. A különböző programeseményekhez különböző hangok tartoznak. Új hangokat a Windows Vezérlőpult Hangok lapján tud az eseményekhez rendelni, a kiválasztás törlésével pedig le tudja tiltani a hangvisszajelzést.

  - **A beolvasási minőség visszajelzésének megmutatása**

    Jelölje be a négyzetet, ha meg szeretné nézni a beolvasott ujjlenyomatokat, azok minőségétől függetlenül.

    Törölje a jelölést, ha csak a jó minőségű beolvasásokat szeretné megnézni.

Az adatok biztonsági mentése és visszaállítása

Azt javasoljuk, hogy a Security Managerben tárolt adatokról rendszeresen készítsen biztonsági másolatot. A biztonsági mentés gyakorisága az adatok módosulásának gyakoriságától függ. Ha pl. naponta ad hozzá új bejelentkezéseket, az adatokról is naponta készítsen biztonsági másolatot.

A biztonsági másolatokat más számítógépre is át lehet helyezni: a folyamat másik neve az exportálás, illetve importálás.

MEGJEGYZÉS: Ez a funkció csak az adatoktól készít biztonsági másolatot.

A HP ProtectTools Security Managert az az összes olyan számítógépre telepíteni kell, amelyre rákerülnek a biztonsági másolatok, mielőtt az adatokat vissza lehetne állítani a biztonsági mentési fájlból.

Az adatok biztonsági mentése:

1. A bal ablaktáblán kattintson a **Speciális**, majd a **Biztonsági mentés és visszaállítás** elemre.
2. Kattintson az **Adatok biztonsági mentése** parancsra.
3. Válassza ki a biztonsági mentésben részt vevő modulokat. A legtöbb esetben az összeset ki kell választani.
4. Adjon meg egy fájlnevet a tároló fájl számára. Alapértelmezés szerint a fájl a Dokumentumok mappában mentődik le. Ha más célhelyet kíván megadni neki, kattintson a **Tallózás** gombra.
5. Adjon meg egy jelszót a fájl védelméhez.
6. Azonosítsa magát.
7. Kattintson a **Kész** gombra.

Az adatok visszaállítása:

1. A bal ablaktáblán kattintson a **Speciális**, majd a **Biztonsági mentés és visszaállítás** elemre.
2. Kattintson az **Adatok visszaállítása** gombra.
3. Válassza ki az előbb létrehozott tároló fájlt. Az útvonalat írja a megjelenő mezőbe, vagy kattintson a **Browse** (Tallózás) parancsra.
4. Adja meg a a fájl védelméhez használt jelszót.
5. Válassza ki a visszaállítani kívánt modulokat. A legtöbb esetben az összeset fel kell sorolni.
6. Kattintson a **Kész** gombra.

Bővebben

Lehetséges, hogy a programot új funkciókkal bővítő kiegészítő alkalmazások is rendelkezésre állnak.

A Security Manager műszerfalán kattintson a **[+] Bővebben** elemre a kiegészítő alkalmazások közötti tallózáshoz.

MEGJEGYZÉS: Ha a műszerfal bal alsó részén nem látható a **[+] Bővebben** hivatkozás, azt a számítógép rendszergazdája tiltotta le.

Frissítések és üzenetek

1. Ha információt szeretne kérni az új alkalmazásokról és frissítésekről, jelölje be a **Keep me informed about new applications and updates** (Értesítést kérek az új alkalmazásokról és frissítésekről) melletti négyzetet.
2. Az automatikus frissítések menetrendjének beállításához adja meg a napok számát.
3. Frissítéseket a **Check Now** (Ellenőrzés) gombra kattintva kereshet.

A biztonsági alkalmazások állapota

A Security Managerben található Az alkalmazások állapota lapon látható a feltelepített biztonsági alkalmazások általános állapota. A lapon a telepített alkalmazások és azok telepítési állapota látható. Az összegzés automatikusan megjelenik, amikor megnyitja a Security Manager kezelőpaneljét, és rákattint a képernyő jobb oldalán lévő Windows eszköztáron található **A biztonsági alkalmazások állapotának ellenőrzése** pontra, a **Biztonsági alkalmazások** pontra vagy az **Ellenőrizze most** parancsra a **Készülék** ikonján.

8 Drive Encryption for ProtectTools szolgáltatás (csak egyes típusokon)

△ **VIGYÁZAT!** Ha a Drive Encryption modul eltávolítása mellett dönt, először vissza kell fejtenie az összes titkosított meghajtót. Ha ezt nem teszi meg, nem tudja elérni a titkosított meghajtón tárolt adatokat, kivéve, ha regisztrált a Drive Encryption helyreállító szolgáltatásra. A Drive Encryption modul újbóli telepítése nem engedélyezi a titkosított meghajtók elérését.

A Drive Encryption for HP ProtectTools modul a számítógép merevlemezének titkosításával teljes körű adatvédelmet biztosít. A Drive Encryption bekapcsolt állapotában be kell jelentkeznie a Drive Encryption bejelentkező képernyőjén, amely még a Windows® operációs rendszer betöltése előtt megjelenik.

A HP ProtectTools telepítő varázsló segítségével a rendszergazdák bekapcsolhatják a Drive Encryption alkalmazást, biztonsági másolatot készíthetnek a titkosító kódról, felhasználókat vehetnek fel és törölhetnek, illetve kikapcsolhatják a Drive Encryption alkalmazást. További információt a HP ProtectTools Security Manager szoftversúgója tartalmaz.

A Drive Encryption alkalmazás az alábbi feladatokat látja el:

- Titkosításkezelés

  Egyedi meghajtók titkosítása vagy dekódolása

  MEGJEGYZÉS: Titkosítani csak a belső meghajtókat lehet.

- Helyreállítás
  - Biztonsági mentési kódok létrehozása
  - Helyreállítás végrehajtása

Beállítási eljárások

A Drive Encryption alkalmazás megnyitása

1. Kattintson a **Start**, a **Minden program**, a **HP**, majd a **HP ProtectTools Administrative Console** elemre.
2. A bal oldali ablaktáblán kattintson a **Drive Encryption** elemre.

Általános feladatok

A Drive Encryption alkalmazás bekapcsolása

A Drive Encryption alkalmazást a HP ProtectTools telepítő varázsló segítségével kapcsolja be.

MEGJEGYZÉS: A varázsló a felhasználók felvétele és törlése során is használható.

– vagy –

1. Kattintson a **Start**, a **Minden program**, a **HP**, majd a **HP ProtectTools Administrative Console** elemre.
2. A bal oldali ablaktáblán kattintson a **Biztonság** majd a **Funkciók** elemre.
3. Jelölje be a **Drive Encryption** négyzetet, majd kattintson a **Tovább** gombra.
4. A **Titkosítandó meghajtók** lehetőség alatt jelölje be a titkosítani kívánt meghajtók melletti négyzetet.
5. Illessze az adathordozó eszközt a megfelelő bővítőhelyre.

   MEGJEGYZÉS: A titkosító kódot csak USB-alapú, FAT32-formátumú adathordozó eszközre lehet elmenteni.

6. Az **Az a külső adathordozó eszköz, amelyre a titkosító kódot el kell menteni** lehetőség alatt válassza ki azt az adathordozó eszközt, amelyre a titkosító kódot menti.
7. Kattintson az **Alkalmaz** elemre.

   Megkezdődik a meghajtó titkosítása.

További információt a HP ProtectTools Security Manager szoftversúgója tartalmaz.

A Drive Encryption alkalmazás kikapcsolása

A Drive Encryption alkalmazást a HP ProtectTools telepítő varázsló segítségével kapcsolja ki. További információt a HP ProtectTools Security Manager szoftversúgója tartalmaz.

– vagy –

1. Kattintson a **Start**, a **Minden program**, a **HP**, majd a **HP ProtectTools Administrative Console** elemre.
2. A bal oldali ablaktáblán kattintson a **Biztonság** majd a **Funkciók** elemre.
3. Törölje a **Drive Encryption** négyzetben lévő jelölést, majd kattintson az **Alkalmaz** gombra.

   Megkezdődik a meghajtó dekódolása.

Bejelentkezés a Drive Encryption alkalmazás bekapcsolása után

Ha a számítógépet akkor kapcsolja be, amikor a Drive Encryption alkalmazás aktív, és az Ön felhasználói fiókja rögzítésre került, a Drive Encryption bejelentkezési képernyőjén keresztül kell bejelentkeznie:

MEGJEGYZÉS: Ha a Windows rendszergazda bekapcsolta a Pre-boot Security alkalmazást a HP ProtectTools Security Managerben, a bejelentkezés a számítógép bekapcsolása után azonnal a számítógépre, nem pedig a Drive Encryption bejelentkezési képernyőjén keresztül történik.

1. Kattintson a felhasználónévre, adja meg Windows-jelszavát vagy a Java™-kártya PIN-kódját, vagy húzza végig a rendszerben rögzített ujját az olvasón.
2. Kattintson az **OK** gombra.

MEGJEGYZÉS: Ha a Drive Encryption bejelentkezési képernyőjén helyreállítási kód segítségével lép be, a rendszer arra is felszólítja, hogy a Windows bejelentkezési képernyőn adja meg Windows-felhasználónevét és jelszavát.

Adatvédelem a merevlemez titkosításával

A merevlemez titkosításával történő adatvédelem biztosításához használja a HP ProtectTools telepítő varázslót:

1. A Security Manager alkalmazásban kattintson az **Első lépések**, majd a **Security Manager beállítása** ikonra. Elindul egy, a Security Manager funkcióit szemléltető bemutató. (A Security Managert a Drive Encryption oldalról is elindíthatja.)
2. A bal oldali ablaktáblán kattintson a **Drive Encryption**, majd a **Titkosításkezelés** elemre.
3. Kattintson a **Titkosítás módosítása** elemre.
4. Válassza ki a titkosítani kívánt meghajtó(ka)t.

MEGJEGYZÉS: Azt javasoljuk, hogy mindenképpen a merevlemezt titkosítsa.

A titkosítási állapot megjelenítése

A titkosítási állapotot a felhasználók a HP ProtectTools Security Manager alkalmazásban tekinthetik meg.

MEGJEGYZÉS: A titkosítási állapotot csak a HP ProtectTools Administrative Console segítségével lehet módosítani.

1. Nyissa meg a **HP ProtectTools Security Manager** alkalmazást.
2. A **Saját adatok** pont alatt kattintson a **Titkosítási állapot** elemre.

   Ha a Drive Encryption be van kapcsolva, a meghajtó állapotát az alábbi állapotkódok jelzik:

   - Aktív
   - Inaktív
   - Nincs titkosítva
   - Titkosított
   - Titkosítása folyamatban
   - Dekódolása folyamatban

   Ha a merevlemez éppen titkosítva vagy dekódolva van, az állapotot egy folyamatsáv jelöli, százalékban, amely a titkosítás vagy dekódolás befejezéséhez szükséges hátralévő időt is mutatja.

Speciális feladatok

A Drive Encryption kezelése (a rendszergazda feladata)

A Titkosításkezelés” oldalon a rendszergazdák megtekinthetik és módosíthatják a Drive Encryption alkalmazás állapotát (be- vagy kikapcsolva), illetve megtekinthetik valamennyi, a számítógépben lévő merevlemez titkosítási állapotát.

- Ha az állapot Inaktív, a Windows rendszergazda még nem kapcsolta be Drive Encryption alkalmazást a HP ProtectTools Security Managerben, így az nem védi merevlemezt. A Drive Encryption alkalmazást a HP ProtectTools Security Manager telepítő varázsló segítségével kapcsolja be.
- Ha az állapot Aktív, a Drive Encryption alkalmazás be van kapcsolva és konfigurálva van. A meghajtó az alábbi állapotok valamelyikében van:
  - Nincs titkosítva
  - Titkosított
  - Titkosítása folyamatban
  - Dekódolása folyamatban

Egyedi meghajtók titkosítása vagy dekódolása

Ha egy vagy több merevlemezt is titkosítani szeretne a számítógépen, vagy egy már titkosított meghajtót szeretne dekódolni, használja a Titkosítás módosítása funkciót:

1. Nyissa meg a **HP ProtectTools Administrative Console** alkalmazást, majd kattintson a **Drive Encryption**, végül pedig a **Titkosításkezelés** lehetőségre.
2. Kattintson a **Titkosítás módosítása** elemre.
3. A Titkosítás módosítása párbeszédpanelen jelölje be a titkosítani vagy dekódolni kívánt merevlemezek melletti négyzetet (vagy vegye ki belőlük a jelölést), majd kattintson az **OK** gombra.

MEGJEGYZÉS: A meghajtó titkosításakor vagy visszafejtésekor a folyamatsáv mutatja a feladat befejezéséből hátralévő időt. Ha a titkosítási folyamat közben a számítógép kikapcsol, illetve alvó vagy hibernált állapotot kezdeményez és újraindul, a Hátralévő idő ábra visszaáll a folyamat elejére, a titkosítás azonban onnan folytatódik, ahol legutóbb abbamaradt. A hátralévő időt jelző, illetve a folyamatot mutató ábra gyorsabban változik, hogy tükrözze a korábbi folyamatot.

Biztonsági mentés és helyreállítás (a rendszergazda feladata)

A rendszergazdák a Recovery (Helyreállítás) oldalon tudnak biztonsági mentést és helyreállítást végezni a titkosító kódokról.

A helyi meghajtó titkosító kódjának biztonsági mentése: a segítségével a titkosító kódról a Drive Encryption alkalmazás bekapcsolt állapotában biztonsági mentés készíthető egy cserélhető adathordozóra.

Biztonsági mentési kódok létrehozása

A titkosított meghajtóhoz készült titkosító kódról így tud biztonsági mentést végezni egy cserélhető adathordozó eszközre:

△ **VIGYÁZAT!** Győződjön meg róla, hogy a biztonsági mentési kódot tartalmazó adathordozó eszköz biztonságos helyen van-e, mert ha elfelejti a jelszót, vagy elveszíti a Java-kártyát, a merevlemezhez csak az adathordozó eszköz segítségével tud hozzáférni.

1. Nyissa meg a **HP ProtectTools Administrative Console** alkalmazást, majd kattintson a **Drive Encryption**, végül pedig a **Helyreállítás** lehetőségre.
2. Kattintson a **Biztonsági mentési kódok** lehetőségre.
3. A Select Backup Disk (Biztonsági mentéshez használt lemez kiválasztása) oldalon jelölje be az ahhoz az eszköz tartozó négyzetet, ahová a titkosító kód biztonsági másolatát menteni szeretné, majd kattintson a **Next** (Tovább) gombra.
4. Olvassa el a következő oldalon látható információt, majd kattintson a **Tovább** gombra. A titkosító kód az Ön által megadott adathordozó eszközre mentődik.
5. A megerősítést kérő párbeszédpanel megnyílása után kattintson a **Befejezés** gombra.

Helyreállítás végrehajtása

Ha elfelejtette a jelszavát, és helyreállítást kell végeznie, tegye a következőket:

1. Kapcsolja be a számítógépet.
2. Csatlakoztassa a biztonsági mentési kódot tartalmazó cserélhető adathordozót.
3. A Drive Encryption for HP ProtectTools bejelentkező párbeszédpaneljének megnyílásakor kattintson a **Mégse** gombra.
4. Kattintson a képernyő bal alsó sarkában látható **Beállítások**, majd a **Helyreállítás** elemre.
5. Válassza ki a biztonsági mentési kódot tartalmazó fájlt, vagy kattintson a **Tallózás** elemre, hogy megkeresse. Ezután kattintson a **Tovább** gombra.
6. A megerősítést kérő párbeszédpanel megnyílása után kattintson az **OK** gombra.

   A számítógép elindul.

MEGJEGYZÉS: Helyreállítás után azt javasoljuk, hogy állítsa vissza a jelszót.

9 Privacy Manager for HP ProtectTools (csak egyes típusokon)

A Privacy Manager for HP ProtectTools segítségével speciális biztonsági belépési (hitelesítési) eljárásokat alkalmazhat a kommunikáció forrásának, épségének és biztonságának ellenőrzésére e-mailezés, Microsoft® Office dokumentumok vagy azonnali üzenetküldő alkalmazások használata közben.

A Privacy Manager kihasználja a HP ProtectTools Security Manager által nyújtott biztonsági infrastruktúrát, amely az alábbi biztonsági bejelentkezési eljárásokat tartalmazza:

- Ujjlenyomat-hitelesítés
- Windows®-jelszó
- HP ProtectTools Java™-kártya

A Privacy Manager szoftverben a fent felsoroltak közül bármelyik biztonsági bejelentkezési eljárást használhatja.

A Privacy Manager rendszerkövetelményei a következők:

- HP ProtectTools Security Manager 5.00 vagy újabb
- Windows® 7, Windows Vista® vagy Windows XP operációs rendszer
- Microsoft Outlook 2007 vagy Microsoft Outlook 2003
- Érvényes e-mail cím

MEGJEGYZÉS: A Privacy Manager biztonsági funkcióit csak egy, a Privacy Managerben igényelt és telepített Privacy Manager-tanúsítvánnyal (egy digitális tanúsítvánnyal) lehet igénybe venni. Privacy Manager-tanúsítvány igényléséről itt olvashat bővebben: Privacy Manager-tanúsítvány igénylése és telepítése, 48. oldal.

Beállítási eljárások

A Privacy Manager megnyitása

A Privacy Manager megnyitása:

1. Kattintson a **Start**, a **Minden program**, a **HP**, majd a **HP ProtectTools Security Manager** lehetőségre.
2. Kattintson a **Privacy Manager** elemre.

– vagy –

A jobb egérgombbal kattintson a tálca jobb oldalán található értesítési területen látható **HP ProtectTools** ikonra, válassza a **Privacy Manager** lehetőséget, végül pedig kattintson a **Konfiguráció** elemre.

– vagy –

Egy Microsoft Outlook e-mail üzenet eszköztárában kattintson a **Biztonságos küldés** elem melletti lefelé nyílra, majd a **Tanúsítványok** vagy a **Megbízható kapcsolatok** elemre.

– vagy –

Egy Microsoft Outlook dokumentum eszköztárában kattintson az **Aláírás és titkosítás** elem melletti lefelé nyílra, majd a **Tanúsítványok** vagy a **Megbízható kapcsolatok** elemre.

A Privacy Manager-tanúsítványok kezelése

A Privacy Manager-tanúsítványok a nyilvános kulcsú adatvédelmi infrastruktúra (PKI) elnevezésű kriptográfiai technológia segítségével védik az adatokat és az üzeneteket. A PKI kriptográfiai kulcsok, valamint egy tanúsító hatóság által kiállított Privacy Manager-tanúsítvány meglétét követeli meg a felhasználóktól. A legtöbb adattitkosító és hitelesítő szoftvertől eltérően, amelyek mindössze rendszeresen hitelesítést kívánnak meg a felhasználóktól, a Privacy Manager minden alkalommal hitelesítésre szólítja fel, ha Ön egy titkosító kód használatával e-mail üzenetet vagy Microsoft Office dokumentumot ír alá. A Privacy Manager stabil és biztonságos információmentést és -küldést nyújt.

Ön az alábbi feladatokat hajthatja végre:

- Privacy Manager-tanúsítványok igénylése és telepítése
- A Privacy Manager-tanúsítvány adatainak megtekintése
- A Privacy Manager-tanúsítványok megújítása
- Egy alapértelmezett Privacy Manager-tanúsítvány beállítása, amelyet a Privacy Manager használni fog, ha több tanúsítvány is rendelkezésre áll
- Privacy Manager-tanúsítványok törlése és visszavonása (haladó)

Privacy Manager-tanúsítvány igénylése és telepítése

A Privacy Manager funkcióinak használatához egy érvényes e-mail címen igényelnie és telepítenie kell egy Privacy Manager-tanúsítványt (a Privacy Managerben). A e-mail címnek a Microsoft Outlookon belüli fióknak kell lennie, ugyanazon a számítógépen, amelyről a Privacy Manager-tanúsítványt igényelte.

Privacy Manager-tanúsítvány igénylése

1. Nyissa meg a Privacy Managert, és kattintson a **Tanúsítványok** elemre.
2. Kattintson a **Privacy Manager-tanúsítvány igénylése** lehetőségre.
3. Olvassa el a szöveget az üdvözlőlapon, majd kattintson a **Next** (Tovább) gombra.
4. Olvassa el a licencszerződést a License Agreement (Licencszerződés) oldalon.
5. Győződjön meg róla, hogy bejelölte-e a **Jelölje be, ha elfogadja a jelen licencszerződés feltételeit** felirat melletti négyzetet, majd kattintson a **Tovább** gombra.
6. Adja meg a kívánt információt a Your Certificate Details (Tanúsítványadatok) oldalon, és kattintson a **Next** (Tovább) gombra.
7. Kattintson a **Befejezés** gombra „A tanúsítványigénylés elfogadva” oldalon.
8. A tanúsítvány bezárásához kattintson az **OK** gombra.

A Privacy Manager-tanúsítványt egy, a Microsoft Outlookba küldött e-mail csatolmányaként kapja meg.

Előre hozzárendelt Privacy Manager vállalati tanúsítvány kérése

1. Nyissa meg azt az e-mailt az Outlookban, amely tartalmazza, hogy a vállalati tanúsítványt Önhöz rendelték.
2. Kattintson a **Kérés** elemre.
3. A Privacy Manager-tanúsítványt egy, a Microsoft Outlookba küldött e-mail csatolmányaként kapja meg.
4. A tanúsítvány telepítéséről itt olvashat bővebben: Privacy Manager-tanúsítvány telepítése, 49. oldal

Privacy Manager-tanúsítvány telepítése

1. Amikor megérkezik a Privacy Manager-tanúsítványt tartalmazó e-mail, nyissa meg, és kattintson a **Telepítés** gombra, amely az Outlook 2007-ben a jobb alsó, az Outlook 2003-ban pedig a jobb felső sarokban található.
2. Igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.
3. A Certificate Installed (A tanúsítvány telepítése kész) oldalon kattintson a **Next** (Tovább) gombra.
4. A Certificate Backup (A tanúsítvány biztonsági mentése) oldalon adja meg a biztonsági mentési fájl célhelyét és nevét, vagy kattintson a **Browse** (Tallózás) elemre, hogy célhelyet keressen neki.

△ **VIGYÁZAT!** Ügyeljen rá, hogy a fájl semmiképpen ne a merevlemezre mentődjön. Tegye biztonságos helyre. A fájlt kizárólag Ön használhatja. Akkor van rá szükség, ha a Privacy Manager-tanúsítványt és a hozzá tartozó kódokat kell visszaállítania.

5. Írjon be és erősítsen meg egy jelszót, majd kattintson a **Tovább** gombra.
6. Igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.
7. Ha úgy dönt, hogy elindítja a Megbízható kapcsolat meghívása folyamatot, kövesse a képernyőn megjelenő utasításokat a 2. lépéstől a következő témakörben: Megbízható kapcsolatok hozzáadása a Microsoft Outlook-névjegyalbum segítségével, 53. oldal .

– vagy –

Ha a **Mégse** elemre kattint, a Megbízható kapcsolatok későbbi hozzáadásáról itt olvashat bővebben: Megbízható kapcsolat hozzáadása, 52. oldal.

A Privacy Manager-tanúsítvány adatainak megtekintése

1. Nyissa meg a Privacy Managert, és kattintson a **Tanúsítványok** elemre.
2. Kattintson a Privacy Manager-tanúsítványra.
3. Kattintson a **Tanúsítványadatok** lehetőségre.
4. Ha végzett az adatok megtekintésével, kattintson az **OK** gombra.

Privacy Manager-tanúsítvány megújítása

Ha a Privacy Manager-tanúsítvány érvényessége a végéhez közeledik, a rendszer felszólítja Önt, hogy újítsa meg:

1. Nyissa meg a Privacy Managert, és kattintson a **Tanúsítványok** elemre.
2. Kattintson a **Tanúsítvány megújítása** lehetőségre.
3. Új Privacy Manager-tanúsítvány vásárlásához kövesse a képernyőn megjelenő utasításokat.

MEGJEGYZÉS: A Privacy Manager-tanúsítvány megújítása nem váltja ki a régi Privacy Manager-tanúsítványt. Önnek új Privacy Manager-tanúsítványt kell vásárolnia és telepítenie, az alábbi részben leírtak szerint: Privacy Manager-tanúsítvány igénylése és telepítése, 48. oldal.

Alapértelmezett Privacy Manager-tanúsítvány megadása

A Privacy Manager alkalmazásban kizárólag a Privacy Manager-tanúsítványok láthatók, hiába telepített további, más tanúsító hatóságok által kiadott tanúsítványokat a számítógépre.

Ha a számítógépen több, a Privacy Managerrel telepített Privacy Manager-tanúsítvány is található, Ön megadhat közülük egy alapértelmezett példányt:

1. Nyissa meg a Privacy Managert, és kattintson a **Tanúsítványok** elemre.
2. Kattintson az alapértelmezettként használni kívánt Privacy Manager-tanúsítványra, majd a **Beállítás alapértelmezettként** parancsra.
3. Kattintson az **OK** gombra.

MEGJEGYZÉS: Az alapértelmezett Privacy Manager-tanúsítvány használata nem kötelező. A Privacy Manager számon funkciója közül Ön bármelyik Privacy Manager-tanúsítványt kiválaszthatja és használhatja.

Privacy Manager-tanúsítvány törlése

Ha töröl egy Privacy Manager-tanúsítványt, a továbbiakban semmilyen, az adott tanúsítvány segítségével titkosított fájlhoz vagy adathoz sem tud hozzáférni. Ha véletlenül kitörölt egy Privacy Manager-tanúsítványt, a tanúsítvány telepítése során létrehozott biztonsági mentési fájlból vissza tudja állítani. További tudnivalók itt olvashatók: Privacy Manager-tanúsítvány visszaállítása, 51. oldal.

Privacy Manager-tanúsítvány törlése:

1. Nyissa meg a Privacy Managert, és kattintson a **Tanúsítványok** elemre.
2. Kattintson a törölni kívánt Privacy Manager-tanúsítványra, majd a **Speciális** elemre.
3. Kattintson a **Törlés** gombra.
4. A megerősítést kérő párbeszédpanel megnyílása után kattintson az **Igen** gombra.
5. Kattintson a **Bezár**, majd az **Alkalmaz** gombra.

Privacy Manager-tanúsítvány visszaállítása

A Privacy Manager-tanúsítvány telepítése során Önnek biztonsági másolatot kell készítenie a tanúsítványról. Biztonsági másolatot a Migráció oldalon is kell készítenie. Ezt a biztonsági másolatot akkor tudja használni, ha áttelepíti az adatokat egy másik számítógépre, vagy ha visszaállít egy tanúsítványt ugyanazon a számítógépen.

1. Nyissa meg a Privacy Managert, és kattintson a **Migráció** elemre.
2. Kattintson a **Visszaállítás** gombra.
3. A Migration File (Migrációs fájl) oldalon kattintson a **Browse** (Tallózás) elemre, hogy megtalálja a .dppsm kiterjesztésű fájlt, amelyet a biztonsági mentés során hozott létre. Ezután pedig kattintson a **Next** (Tovább) gombra.
4. Adja meg a biztonsági mentés során használt jelszót, majd kattintson a **Tovább** elemre.
5. Kattintson a **Kész** gombra.
6. Kattintson az **OK** gombra.

További tudnivalókat itt: Privacy Manager-tanúsítvány telepítése, 49. oldal, illetve itt: A Privacy Manager-tanúsítványok és a Megbízható kapcsolatok biztonsági mentése, 67. oldal olvashat.

Privacy Manager-tanúsítvány visszavonása

Ha úgy érzi, hogy a Privacy Manager-tanúsítvány biztonsága megsérült, visszavonhatja a tanúsítványt:

MEGJEGYZÉS: A visszavont Privacy Manager-tanúsítvány nem minősül töröltnek. A tanúsítvány továbbra is használható a vele titkosított fájlok megtekintésére.

1. Nyissa meg a Privacy Managert, és kattintson a **Tanúsítványok** elemre.
2. Kattintson a **Speciális** elemre.
3. Kattintson a visszavonni kívánt Privacy Manager-tanúsítványra, majd a **Visszavonás** elemre.
4. A megerősítést kérő párbeszédpanel megnyílása után kattintson az **Igen** gombra.
5. Igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.
6. Kövesse a képernyőn megjelenő utasításokat.

A Megbízható kapcsolatok kezelése

A Megbízható kapcsolatok azok a felhasználók, akikkel Ön Privacy Manager-tanúsítványt cserélt, így lehetővé vált az egymás közötti biztonságos kommunikáció.

A Megbízható kapcsolatok kezelése lapon a következő feladatok végezhetők el:

- A Megbízható kapcsolatok adatainak megtekintése
- A Megbízható kapcsolatok törlése
- A Megbízható kapcsolatok visszavont állapotának ellenőrzése (haladó)

Megbízható kapcsolatok hozzáadása

A Megbízható kapcsolatok hozzáadása 3 lépésből áll:

1. Ön e-mailben meghívja a Megbízható kapcsolat címzettjét.
2. A Megbízható kapcsolat címzettje válaszol az e-mailre.
3. Ön megkapja a Megbízható kapcsolatok címzettjének válaszát. Ezután kattintson az **Elfogadás** elemre.

Ön egyesével is meghívhat e-mailben személyeket a Megbízható kapcsolatok közé, vagy a meghívást a Microsoft Outlook címjegyzékben szereplő valamennyi kapcsolatnak is elküldheti.

Megbízható kapcsolatokat az alábbi szakaszokban leírtaknak megfelelően adhat hozzá.

MEGJEGYZÉS: Hogy valaki el tudja fogadni a Megbízható kapcsolatok közé szóló meghívást, ahhoz vagy a Privacy Managerrel, vagy egy alternatív klienssel kell rendelkeznie a számítógépen. Az alternatív kliens telepítéséről a DigitalPersona webhelyén, a http://DigitalPersona.com/PrivacyManager címen olvashat bővebben.

Megbízható kapcsolat hozzáadása

1. Nyissa meg a Privacy Managert, és kattintson a **Megbízható kapcsolatok kezelése**, majd a **Kapcsolatok meghívása** elemre.

   – vagy –

   A Microsoft Outlook eszköztárában kattintson a **Biztonságos küldés** elem melletti lefelé nyílra, majd a **Kapcsolatok meghívása** lehetőségre.

2. Ha megnyílik a Tanúsítvány küldése párbeszédpanel, kattintson a használni kívánt Privacy Manager-tanúsítványra, majd az **OK** gombra.
3. A Megbízható kapcsolat meghívása párbeszédpanel megnyílása után olvassa el a szöveget, majd kattintson az **OK** gombra.

   Ez után automatikusan készül egy e-mail.

4. Adja meg azon címzett(ek) e-mail címét, aki(ke)t fel kíván venni a Megbízható kapcsolatok közé.
5. Szerkessze a szöveget és írja alá a levelet (ha kívánja).
6. Kattintson a **Küldés** gombra.

   MEGJEGYZÉS: Ha nem kapott Privacy Manager-tanúsítványt, a rendszer üzenetben értesíti, hogy Megbízható kapcsolat igényléséhez Privacy Manager-tanúsítvánnyal kell rendelkeznie. A Tanúsítványigénylő varázsló elindításához kattintson az **OK** gombra. További tudnivalók itt olvashatók: Privacy Manager-tanúsítvány igénylése és telepítése, 48. oldal.

7. Igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.

MEGJEGYZÉS: Ha a Megbízható kapcsolatként megjelölt címzett megkapta az e-mailt, meg kell nyitnia, és az e-mail jobb alsó sarkában látható **Elfogadás** elemre, majd a megerősítést kérő párbeszédpanel megjelenése után az **OK** gombra kell kattintania.

8. Ha valamelyik, a Megbízható kapcsolatok közé meghívott címzett jóváhagyó e-mailt küld Önnek, kattintson az e-mail jobb alsó sarkában látható **Elfogadás** elemre.

   Megjelenik egy, a címzettnek a Megbízható kapcsolatok közé történő felvételéről tájékoztató párbeszédablak.

9. Kattintson az **OK** gombra.

Megbízható kapcsolatok hozzáadása a Microsoft Outlook-névjegyalbum segítségével

1. Nyissa meg a Privacy Managert, és kattintson a **Megbízható kapcsolatok kezelése**, majd a **Kapcsolatok meghívása** elemre.

   – vagy –

   A Microsoft Outlook eszköztárában kattintson a **Biztonságos küldés** elem melletti lefelé nyílra, majd a **Az Outlook-névjegyalbumban lévő összes kapcsolat meghívása** lehetőségre.

2. A Trusted Contact Invitation (Megbízható kapcsolat meghívása) oldal megnyílása után válassza ki a Trusted Contacts (Megbízható kapcsolatok) közé felvenni kívánt címzettek e-mail címét, és kattintson a **Next** (Tovább) gombra.

3. A Sending Invitation (Meghívás küldése) oldal megnyílása után kattintson a **Finish** (Kész) gombra.

   Automatikusan létrejön egy, a Microsoft Outlookban tárolt kiválasztott e-mail címeket tartalmazó levelezőlista.

4. Szerkessze a szöveget és írja alá a levelet (ha kívánja).

5. Kattintson a **Küldés** gombra.

MEGJEGYZÉS: Ha nem kapott Privacy Manager-tanúsítványt, a rendszer üzenetben értesíti, hogy Megbízható kapcsolat igényléséhez Privacy Manager-tanúsítvánnyal kell rendelkeznie. A Tanúsítványigénylő varázsló elindításához kattintson az **OK** gombra. További tudnivalók itt olvashatók: Privacy Manager-tanúsítvány igénylése és telepítése, 48. oldal .

6. Igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.

MEGJEGYZÉS: Ha a Megbízható kapcsolatként megjelölt címzett megkapta az e-mailt, meg kell nyitnia, és az e-mail jobb alsó sarkában látható **Elfogadás** elemre, majd a megerősítést kérő párbeszédpanel megjelenése után az **OK** gombra kell kattintania.

7. Ha valamelyik, a Megbízható kapcsolatok közé meghívott címzett jóváhagyó e-mailt küld Önnek, kattintson az e-mail jobb alsó sarkában látható **Elfogadás** elemre.

   Megjelenik egy, a címzettnek a Megbízható kapcsolatok közé történő felvételéről tájékoztató párbeszédablak.

8. Kattintson az **OK** gombra.

A Megbízható kapcsolatok adatainak megtekintése

1. Nyissa meg a Privacy Managert, és kattintson a **Megbízható kapcsolatok** elemre.

2. Kattintson az egyik Megbízható kapcsolatra.

3. Kattintson a **Kapcsolatadatok** lehetőségre.
4. Ha végzett az adatok megtekintésével, kattintson az **OK** gombra.

Megbízható kapcsolat törlése

1. Nyissa meg a Privacy Managert, és kattintson a **Megbízható kapcsolatok** elemre.
2. Kattintson a törölni kívánt Megbízható kapcsolatra.
3. Kattintson a **Kapcsolat törlése** gombra.
4. A megerősítést kérő párbeszédpanel megnyílása után kattintson az **Igen** gombra.

Megbízható kapcsolat visszavont állapotának ellenőrzése

Ha látni szeretné, hogy egy Megbízható kapcsolat visszavonta-e a Privacy Manager-tanúsítványát:

1. Nyissa meg a Privacy Managert, és kattintson a **Megbízható kapcsolatok** elemre.
2. Kattintson az egyik Megbízható kapcsolatra.
3. Kattintson a **Speciális** gombra.

   Megnyílik a Megbízható kapcsolatok speciális kezelése párbeszédpanel.
4. Kattintson a **Visszavonás ellenőrzése** lehetőségre.
5. Kattintson a **Bezárás** gombra.

Általános feladatok

A Privacy Manager az alábbi Microsoft termékekhez használható:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

A Privacy Manager használata a Microsoft Outlook programban

A Privacy Manager feltelepítése után a Microsoft Outlook eszköztárában megjelenik egy Adatvédelem, a Microsoft Outlookban írt e-mailek eszköztárában pedig egy Biztonságos küldés feliratú gomb. Ha az **Adatvédelem** vagy a **Biztonságos küldés** gomb melletti lefelé nyílra kattint, az alábbi lehetőségek közül választhat:

- Aláírás és küldés (csak a Biztonságos küldés gomb esetén): digitális aláírást ad az e-mailhez, és a kiválasztott biztonsági belépési eljárással történő hitelesítés után elküldi.
- Bélyegző a Megbízható kapcsolatokhoz és küldés (csak a Biztonságos küldés gomb esetén): digitális aláírást ad az e-mailhez, titkosítja, majd a kiválasztott biztonsági belépési eljárással történő hitelesítés után elküldi.
- Kapcsolatok meghívása: Megbízható kapcsolatok meghívásának elküldését teszi lehetővé. További tudnivalók itt olvashatók: Megbízható kapcsolat hozzáadása, 52. oldal.
- Az Outlookban lévő kapcsolatok meghívása: Megbízható kapcsolatok meghívásának elküldését teszi lehetővé a Microsoft Outlook névjegyalbumban szereplő összes kapcsolat számára. További tudnivalók itt olvashatók: Megbízható kapcsolatok hozzáadása a Microsoft Outlook-névjegyalbum segítségével, 53. oldal.
- A Privacy Manager megnyitása: a Tanúsítványok, a Megbízható kapcsolatok és a Beállítások lehetőségek segítségével megnyithatja a Privacy Manager alkalmazást, és hozzáadhatja, megtekintheti vagy módosíthatja a meglévő beállításokat. További tudnivalók itt olvashatók: A Privacy Manager konfigurálása a Microsoft Outlookhoz, 55. oldal.

A Privacy Manager konfigurálása a Microsoft Outlookhoz

1. Nyissa meg a Privacy Managert, kattintson a **Beállítások** lehetőségre, majd az **E-mail** lapra.

   – vagy –

   A Microsoft Outlook fő eszköztárában kattintson az **Biztonságos küldés** (az Outlook 2003-ban **Adatvédelem**) elem melletti lefelé nyílra, majd a **Beállítások** elemre.

   – vagy –

   Egy Microsoft e-mail üzenet eszköztárában kattintson a **Biztonságos küldés** elem melletti lefelé nyílra, majd a **Beállítások** elemre.

2. Válassza ki a biztonságos e-mail üzenet küldése során végrehajtani kívánt műveletet, majd kattintson az **OK** gombra.

E-mailek aláírása és küldése

1. A Microsoft Outlookban kattintson az **Új** vagy a **Válasz** elemre.
2. Írja be az e-mail szövegét.
3. Kattintson a **Biztonságos küldés** (az Outlook 2003-ban **Adatvédelem**) elem melletti lefelé nyílra, majd az **Aláírás és küldés** parancsra.
4. Igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.

E-mailek lebélyegzése és küldése

A lebélyegzett e-mailek digitális aláírással és bélyegzővel (titkosítással) rendelkeznek, és csak azok nyithatják meg, akiket Ön kiválaszt a Megbízható kapcsolatok listáról.

E-mail lebélyegzése és elküldése egy Megbízható kapcsolatnak:

1. A Microsoft Outlookban kattintson az **Új** vagy a **Válasz** elemre.
2. Írja be az e-mail szövegét.
3. Kattintson a **Biztonságos küldés** (az Outlook 2003-ban **Adatvédelem**) elem melletti lefelé nyílra, majd az **Lebélyegzés a Megbízható kapcsolatokhoz és küldés** parancsra.
4. Igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.

Lebélyegzett e-mail megtekintése

Ha megnyit egy lebélyegzett e-mailt, az üzenet fejlécében egy biztonsági címke látható. A biztonsági címke az alábbi információkat tartalmazza:

- Az e-mailt aláíró személy azonosságát hitelesítő adatok típusa
- Az e-mailt aláíró személyt hitelesítő adatokat ellenőrző termék neve

A Privacy Manager használata Microsoft Office 2007 dokumentumokban

MEGJEGYZÉS: A Privacy Manager csak Microsoft Office 2007 dokumentumokkal használható.

A Privacy Manager-tanúsítvány hitelesítése után valamennyi Microsoft Word, Microsoft Excel és Microsoft PowerPoint dokumentum eszköztárának jobb oldalán megjelenik az Aláírás és titkosítás gomb. Ha az **Aláírás és titkosítás** gomb melletti lefelé nyílra kattint, az alábbi lehetőségek közül választhat:

- Dokumentumok aláírása: digitális aláírást illeszt a dokumentumba.
- Aláírási sor beillesztése aláírás előtt (kizárólag Microsoft Wordben és Microsoft Excelben): az aláírási sor beillesztésére alapértelmezés szerint Microsoft Word vagy Microsoft Excel dokumentumok aláírása és titkosítása során kerül sor. Ha kiszeretné kapcsolni ezt a beállítást, kattintson az **Aláírási sor hozzáadása** melletti négyzetre, és vegye ki belőle a jelölést.
- Dokumentumok titkosítása: digitális aláírást illeszt a dokumentumba, és titkosítja.
- A titkosítás eltávolítása: eltávolítja a dokumentum titkosítását.
- A Privacy Manager megnyitása: a Tanúsítványok, a Megbízható kapcsolatok és a Beállítások lehetőségek segítségével megnyithatja a Privacy Manager alkalmazást, és hozzáadhatja, megtekintheti vagy módosíthatja a meglévő beállításokat. További tudnivalókat itt: A Privacy

Manager-tanúsítványok kezelése, 48. oldal , A Megbízható kapcsolatok kezelése, 51. oldal , illetve itt: A Privacy Manager konfigurálása a Microsoft Office-hoz, 57. oldal olvashat.

A Privacy Manager konfigurálása a Microsoft Office-hoz

1. Nyissa meg a Privacy Managert, kattintson a **Beállítások** lehetőségre, majd a **Dokumentumok** lapra.

   – vagy –

   Egy Microsoft Office dokumentum eszköztárában kattintson az **Aláírás és titkosítás** elem melletti lefelé nyílra, majd a **Beállítások** elemre.

2. Válassza ki a konfigurálni kívánt alkalmazást, majd kattintson az **OK** gombra.

Microsoft Office dokumentumok aláírása

1. Hozzon létre és mentsen el egy Microsoft Word, Microsoft Excel vagy Microsoft PowerPoint dokumentumot.
2. Kattintson az **Aláírás és titkosítás** gomb melletti lefelé nyílra, majd a **Dokumentum aláírása** lehetőségre.
3. Igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.
4. A megerősítést kérő párbeszédpanel megnyílása után olvassa el a szöveget, majd kattintson az **OK** gombra.

Ha a későbbiekben szerkeszteni kívánja a dokumentumot, tegye a következőket:

1. Kattintson a képernyő bal felső sarkában megjelenő **Office** gombra.
2. Kattintson az **Előkészítés**, majd a **Véglegesként megjelöl** gombra.
3. A megerősítést kérő párbeszédpanel megnyílása után kattintson az **Igen** gombra, és folytassa a munkát.
4. A szerkesztés befejeztével ismét írja alá a dokumentumot.

Aláírási sor hozzáadása Microsoft Word vagy Microsoft Excel dokumentumok aláírása közben

A Privacy Manager segítségével aláírási sort illeszthetnek be a Microsoft Word vagy Microsoft Excel dokumentumok aláírása közben:

1. Hozzon létre és mentsen el egy Microsoft Word vagy Microsoft Excel dokumentumot.
2. Kattintson a **Kezdőlap** menüre.
3. Kattintson az **Aláírás és titkosítás** gomb melletti lefelé nyílra, majd az **Aláírási sor beillesztése aláírás előtt** lehetőségre.

   MEGJEGYZÉS: Az Aláírási sor beillesztése aláírás előtt lehetőség kiválasztása után a szöveg mellett megjelenik egy pipa. A beállítás alapértelmezés szerint be van kapcsolva.

4. Kattintson az **Aláírás és titkosítás** gomb melletti lefelé nyílra, majd a **Dokumentum aláírása** lehetőségre.
5. Igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.

Javasolt aláírók hozzáadása Microsoft Word vagy Microsoft Excel dokumentumokhoz

Javasolt aláírók kijelölésével több aláírási sort is beilleszthet a dokumentumba. A javasolt aláíró olyan felhasználó, akit a Microsoft Word vagy Microsoft Excel dokumentum tulajdonosa jelölt ki, hogy aláírási sort illesszen a dokumentumba. A javasolt aláíró Ön vagy más is lehet, aki alá kívánja írni a dokumentumot. Ha például olyan dokumentumot készít, amelyet az összes az osztályon dolgozó munkatársának alá kell írnia, a dokumentum utolsó oldalának alján készíthet számukra aláírási sorokat, és megmondhatja azt is, hogy pontosan mikor írják alá.

Javasolt aláírók hozzáadása Microsoft Word vagy Microsoft Excel dokumentumokhoz:

1. Hozzon létre és mentsen el egy Microsoft Word vagy Microsoft Excel dokumentumot.
2. Kattintson a **Beszúrás** menüre.
3. Az eszköztár **Szöveg** csoportjában kattintson az **Aláírási sor** felirat melletti nyílra, majd a **Privacy Manager aláírás-szolgáltatás** elemre.

   Ekkor megjelenik az Aláírás beállítás párbeszédpanel.
4. A **Suggested signer** (Javasolt aláíró) mező alatt adja meg a javasolt aláíró nevét.
5. Az **Instructions to the signer** (Az aláírónak szóló utasítások) mező alatt írjon be egy üzenetet az adott javasolt aláírónak.

MEGJEGYZÉS: Az üzenet a cím helyén jelenik meg, és a dokumentum aláírása után vagy törlődik, vagy a másik felhasználó címére cserélődik.

6. A dátum megjelenítéséhez jelölje be az **Aláírás dátumának megjelenítése az aláírási sorban** szöveg melletti négyzetet.
7. A cím megjelenítéséhez jelölje be az **Aláíró címének megjelenítése az aláírási sorban** szöveg melletti négyzetet.

MEGJEGYZÉS: Mivel a dokumentum tulajdonosa javasolt aláírókat rendel a dokumentumhoz, ha az **Aláírás dátumának megjelenítése az aláírási sorban** és/vagy az **Aláíró címének megjelenítése az aláírási sorban** szöveg melletti négyzetek nincsenek bejelölve, a javasolt aláíró akkor sem fogja tudni megjeleníteni a dátumot és/vagy a címet az aláírási sorban, ha az általa használt dokumentumbeállítások ezt lehetővé tennék.

8. Kattintson az **OK** gombra.

Javasolt aláíró aláírási sorának beillesztése

Ha a javasolt aláírók megnyitják a dokumentumot, a nevüket zárójelben látják. Ez hívja fel a figyelmüket arra, hogy alá kell írniuk a dokumentumot.

A dokumentum aláírása:

1. Kattintson duplán a megfelelő aláírási sorra.
2. Igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.

   Az aláírási sor a dokumentum tulajdonosa által megadott módon jelenik meg.

Microsoft Office dokumentumok titkosítása

Ön tud Microsoft Office dokumentumot titkosítani mind a saját maga, mind a Megbízható kapcsolatok számára. Egy dokumentum titkosítása és bezárása után Önnek és a listáról kiválasztott Megbízható kapcsolatoknak a megnyitása előtt hitelesíteniük kell magukat.

Microsoft Office dokumentumok titkosítása:

1. Hozzon létre és mentsen el egy Microsoft Word, Microsoft Excel vagy Microsoft PowerPoint dokumentumot.
2. Kattintson a **Kezdőlap** menüre.
3. Kattintson az **Aláírás és titkosítás** gomb melletti lefelé nyílra, majd a **Dokumentum titkosítása** lehetőségre.

   Megnyílik a Megbízható kapcsolatok kiválasztása párbeszédpanel.
4. Kattintson annak a Megbízható kapcsolatnak a nevére, aki majd megnyithatja és megtekintheti a dokumentumot.

   MEGJEGYZÉS: Több Megbízható kapcsolat nevének kiválasztásához tartsa lenyomva a ctrl billentyűt, és úgy kattintson az egyes nevekre.
5. Kattintson az **OK** gombra.

Ha a későbbiekben szerkeszteni kívánja a dokumentumot, kövesse az ebben részben leírtakat: Titkosítás eltávolítása egy Microsoft Office dokumentumból, 59. oldal . A titkosítás eltávolítása után a dokumentum szerkeszthetővé válik. A dokumentum újratitkosításához kövesse a jelen fejezetben leírtakat.

Titkosítás eltávolítása egy Microsoft Office dokumentumból

Ha eltávolítja a titkosítást egy Microsoft Office dokumentumból, Önnek és a Megbízható kapcsolatoknak a jövőben nem kell hitelesíteniük magukat a dokumentum megnyitásához és megtekintéséhez.

Titkosítás eltávolítása egy Microsoft Office dokumentumból:

1. Nyisson meg egy titkosított Microsoft Word, Microsoft Excel vagy Microsoft PowerPoint dokumentumot.
2. Igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.
3. Kattintson a **Kezdőlap** menüre.
4. Kattintson az **Aláírás és titkosítás** gomb melletti lefelé nyílra, majd a **Titkosítás eltávolítása** lehetőségre.

Titkosított Microsoft Office dokumentum elküldése

Titkosított Microsoft Office dokumentumot úgy is el tud küldeni e-mailben, hogy aláírná vagy titkosítaná magát az e-mailt. Ehhez úgy hozza létre és küldje el az aláírt és titkosított dokumentumot tartalmazó e-mailt, mint ahogy egy normál e-mail és csatolmány esetén tenné.

A maximális biztonság érdekében azonban azt javasoljuk, hogy aláírt és titkosított Microsoft Office dokumentumok esetén magát az e-mailt is titkosítsa.

Lebélyegzett, aláírt és/vagy titkosított Microsoft Office dokumentumot tartalmazó e-mail küldéséhez tegye a következőket:

1. A Microsoft Outlookban kattintson az **Új** vagy a **Válasz** elemre.
2. Írja be az e-mail szövegét.
3. Csatolja a Microsoft Office dokumentumot.
4. További tudnivalókat itt olvashat: E-mailek lebélyegzése és küldése, 56. oldal .

Aláírt Microsoft Office dokumentum megjelenítése

MEGJEGYZÉS: Aláírt Microsoft Office dokumentum megtekintéséhez nincs szükség Privacy Manager-tanúsítványra.

Amikor megnyit egy aláírt Microsoft Office dokumentumot, a dokumentum ablakának alján látható állapotsávban megjelenik egy Digitális aláírás ikon.

1. Kattintson a **Digitális aláírás** ikonra, hogy váltani tudjon az Aláírások párbeszédpanel megjelenítései között. A párbeszédpanel jeleníti meg valamennyi, a dokumentumot aláíró személy nevét, és az egyes aláírások dátumát.
2. Az egyes aláírásokra vonatkozó további adatok megtekintéséhez kattintson a jobb egérgombbal az Aláírások párbeszédpanelre, és válassza ki az Aláírásadatok lehetőséget.

Titkosított Microsoft Office dokumentum megjelenítése

Ha egy titkosított Microsoft Office dokumentumot egy másik számítógépen kíván megjeleníteni, ahhoz arra a számítógépre is telepítenie kell a Privacy Managert. Emellett azt a Privacy Manager-tanúsítványt is vissza kell állítania, amellyel a fájlt titkosították.

A titkosított Microsoft Office dokumentumot megjeleníteni kívánó Megbízható kapcsolatnak Privacy Manager-tanúsítvánnyal kell rendelkeznie, és telepítenie kell a számítógépre a Privacy Managert. Fontos továbbá, hogy a Megbízható kapcsolatot a titkosított Microsoft Office dokumentum tulajdonosának kell kiválasztania.

A Privacy Manager használata a Windows Live Messengerben

A Privacy Manager az alábbi kommunikációs biztonságot biztosító funkciókat nyújtja a Windows Live Messenger programban:

- **Biztonságos csevegés**: az üzenetek SSL/TLS szabvánnyal, XML-protokollal – azaz ugyanazzal az eljárással kerülnek továbbításra, amelyet az online kereskedelmi tranzakciók során használnak.
- **Címzett azonosítása**: Ön már az üzenet elküldése előtt megnézheti, hogy a másik fél gépnél van-e, és a személyazonosságát is ellenőrizheti.
- **Aláírt üzenetek**: Ön elektronikusan aláírhatja az üzeneteit. Ha az üzenetet módosítják, a címzetthez már érvénytelen megjelöléssel jut el.
- **A funkciók elrejtése/megjelenítése**: bármelyik, illetve az összes üzenetet elrejtheti a Privacy Manager Csevegésablakában. Üzenetet úgy is küldhet, hogy a tartalma nem látható. Az üzenet megjelenítéséhez hitelesítésre van szükség.

- **Biztonságos csevegéselőzmények**: az egyes beszélgetések naplófájljai a mentés előtt titkosításra kerülnek, és megjelenítésükhöz hitelesítésre van szükség.
- **Automatikus zárolás/feloldás**: Ön zárolhatja vagy feloldhatja a Privacy Manager Csevegés ablakát – de úgy is beállíthatja, hogy adott ideig tartó tétlenség után automatikusan zárolódjon.

A Privacy Manager Csevegés elindítása

MEGJEGYZÉS: A Privacy Manager Csevegés használatához mindkét félnek telepített Privacy Managerrel és Privacy Manager-tanúsítvánnyal kell rendelkeznie. A Privacy Manager-tanúsítványok telepítéséről itt olvashat bővebben: Privacy Manager-tanúsítvány igénylése és telepítése, 48. oldal.

1. Ha el szeretné indítani a Privacy Manager Csevegés alkalmazást a Windows Live Messengerben, tegye a következőket:

   a. A Live Messengerben kattintson a jobb egérgombbal valamelyik online kapcsolatra, majd válassza a **Tevékenység indítása** lehetőséget.

   b. Kattintson a **Chat indítása** lehetőségre.

   – vagy –

   a. Kattintson duplán valamelyik online ismerősre a Live Messengerben, majd válassza a **Tevékenységek listájának megtekintése** menüt.

   b. Kattintson a **Művelet**, majd a **Chat indítása** elemre.

   – vagy –

   a. A jobb egérgombbal kattintson a **ProtectTools** ikonra az értesítési területen. Ezután kattintson a **Privacy Manager for HP ProtectTools**, majd a **Start Chat** (Csevegés indítása) lehetőségre.

   b. A Live Messengerben kattintson a **Műveletek: Tevékenység indítása**, majd a **Privacy Manager Csevegés** lehetőségre.

   MEGJEGYZÉS: A felhasználóknak bejelentkezve kell lenniük a Live Messenger alkalmazásba, és meg kell jelenniük egymás Live Messenger online ablakában. Kattintson valamelyik online felhasználóra.

   A Privacy Manager meghívja az adott kapcsolatot a Privacy Manager Csevegésbe. Ha a meghívott kapcsolat elfogadja a meghívást, megnyílik a Privacy Manager Csevegés ablaka. Ha a meghívott fél nem rendelkezik Privacy Manager alkalmazással, a rendszer felszólítja, hogy töltse le.

2. A biztonságos csevegés elindításához kattintson a **Start** gombra.

A Privacy Manager konfigurálása a Windows Live Messengerhez

1. Kattintson a **Beállítások** gombra a Privacy Manager Csevegésben.

   – vagy –

   A Privacy Managerben kattintson a **Beállítások** lehetőségre, majd a **Chat** lapra.

   – vagy –

   Kattintson a **Beállítások** gombra a Privacy Manager Live Messenger Csevegéselőzmény-megjelenítőben.

2. Megadhatja, hogy a Privacy Manager Chat (Csevegés) hány perc után fejezze be a beszélgetést. Ehhez válasszon egy számot a **Lock session after _ minutes of activity** (Beszélgetés befejezése _ perc tétlenség után) mezőben.

3. Ha szeretne megadni egy, a csevegéselőzményeket tartalmazó mappát, kattintson a **Tallózás** lehetőségre, és keressen egy megfelelő mappát. Ezután pedig kattintson az **OK** gombra.

4. Ha szeretné, hogy a csevegések végén a naplófájlok titkosítva legyenek és elmentődjenek, jelölje be a **Biztonságos csevegéselőzmények automatikus mentése** négyzetet.

5. Kattintson az **OK** gombra.

Csevegés a Privacy Manager Csevegés ablakában

A Privacy Manager Csevegés elindítása után megnyílik a Privacy Manager Csevegés ablaka a Windows Live Messengerben. A Privacy Manager Csevegés használata megegyezik az egyszerű Windows Live Messengerével. A különbség az, hogy a Privacy Manager Csevegés ablakában az alábbi kiegészítő funkciók is megtalálhatók:

- A **Mentés** gombra kattintva a rendszer a konfigurációs beállításokban megadott mappába menti a beszélgetés tartalmát. A Privacy Manager Csevegés alkalmazást úgy is beállíthatja, hogy kilépés után valamennyi beszélgetést automatikusan elmentse.
- Az **Összes elrejtése**, illetve az **Összes megjelenítése** gombra kattintva összecsukhatja, illetve kibonthatja a Biztonságos kommunikáció ablakban látható üzeneteket. Az egyes üzeneteket a fejlécükre kattintva is elrejtheti vagy megjelenítheti.
- Az **Itt vagy?** gombra kattintva megerősítést kérhet az ismerősétől.
- A **Lezárás** gombra kattintva becsukódik a Privacy Manager Csevegés ablaka, és ismét megnyílik a Csevegés megnyitása ablak. Ha ismét meg kívánja jeleníteni a Biztonságos kommunikáció ablakot, kattintson a **Beszélgetés folytatása** lehetőségre, majd igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.
- A **Küldés** gombra kattintva titkosított üzenetet küldhet az ismerősének.
- A **Küldés aláírással** négyzet bejelölése után üzeneteit elektronikusan aláírva és titkosítva küldheti el. Ha az üzenetet módosítják, a címzetthez már érvénytelen megjelöléssel jut el. Minden aláírással ellátott üzenetet elküldése előtt igazolnia kell magát.
- A **Rejtett küldés** négyzet bejelölése után üzeneteit titkosítva, csak a fejlécet megjelenítve küldheti el. Az üzenet tartalmának elolvasásához az ismerősének igazolnia kell magát.

A csevegéselőzmények megjelenítése

A Privacy Manager Csevegés: a Live Messenger Csevegéselőzmény-megjelenítőben megtekintheti a Privacy Manager Csevegés titkosított előzményeit. A beszélgetéseket vagy a Privacy Manager Csevegés ablakában található **Mentés** lehetőségre kattintva, vagy az automatikus mentésnek a Privacy Manager Csevegés lapján történő beállításával mentheti el. A megjelenítőben minden beszélgetés mellett látható a kapcsolat (titkosított) nyilvános neve, valamint a beszélgetés kezdetének és végének dátuma és időpontja. A beszélgetések alapértelmezett állapotban valamennyi beállított e-mail fiók mellett megjelennek. Ha csak bizonyos fiókokat szeretne megtekinteni, használja a **Fiók előzményeinek megjelenítése** menüt.

A megjelenítőben a következő feladatok végezhetők el:

- Az összes beszélgetés felfedése, 63. oldal
- Egy adott fiókhoz tartozó beszélgetések felfedése, 63. oldal
- A beszélgetés azonosítójának megjelenítése, 64. oldal
- Beszélgetés megjelenítése, 64. oldal
- Adott szövegek keresése a beszélgetések szövegében, 64. oldal
- Beszélgetés törlése, 64. oldal
- Oszlopok hozzáadása vagy törlése, 65. oldal
- A megjelenített beszélgetések szűrése, 65. oldal

A Live Messenger Csevegéselőzmény-megjelenítő megnyitása:

▲ A jobb egérgombbal kattintson az értesítési területen, a tálca jobb szélén található **HP ProtectTools** ikonra, majd kattintson a **Privacy Manager: for HP ProtectTools**, végül pedig a **Live Messenger Csevegéselőzmény-megjelenítő** elemre.

– vagy –

▲ A Csevegésen belül kattintson a **Csevegéselőzmény-megjelenítő** vagy az **Előzmény** lehetőségre.

Az összes beszélgetés felfedése

Az összes beszélgetés megjelenítésével valamennyi, az aktuális beszélgetésben részt vevő ismerős dekódolt neve, és valamennyi, az adott fiókhoz tartozó beszélgetés láthatóvá válik.

Az összes mentett csevegéselőzmény felfedése:

1. A jobb egérgombbal kattintson bármelyik beszélgetésre a Live Messenger Csevegéselőzmény-megjelenítőben, majd válassza **Az összes beszélgetés felfedése** lehetőséget.
2. Igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.

   A kapcsolatok nyilvános neve dekódolva van.
3. A beszélgetésekre duplán kattintva azok tartalmát is elolvashatja.

Egy adott fiókhoz tartozó beszélgetések felfedése

Egy beszélgetés felfedésével az éppen kiválasztott beszélgetésben részt vevő kapcsolat dekódolt nyilvános neve is láthatóvá válik.

Egy adott csevegéselőzmény felfedése:

1. A jobb egérgombbal kattintson bármelyik beszélgetésre a Live Messenger Csevegéselőzmény-megjelenítőben, majd válassza a **Beszélgetés felfedése** lehetőséget.
2. Igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.

   A kapcsolat nyilvános neve dekódolva van.
3. A felfedett beszélgetésekre duplán kattintva azok tartalmát is elolvashatja.

MEGJEGYZÉS: Az ugyanazzal a tanúsítvánnyal titkosított többi beszélgetés mellett egy kioldott lakat ikon látható, amely azt jelzi, hogy ezek közül bármelyiket csak rákattintással, mindben további hitelesítés nélkül el lehet olvasni. A más tanúsítvánnyal titkosított többi beszélgetés mellett egy lezárt lakat ikon látható, amely azt jelzi, hogy a kapcsolatok nyilvános nevének, illetve a tartalom megtekintéséhez további hitelesítés szükséges.

A beszélgetés azonosítójának megjelenítése

A beszélgetés azonosítójának megjelenítése:

- A jobb egérgombbal kattintson bármelyik felfedett beszélgetésre a Live Messenger Csevegéselőzmény-megjelenítőben, majd válassza a **Beszélgetés azonosítójának megjelenítése** lehetőséget.

Beszélgetés megjelenítése

A beszélgetés megjelenítésére megnyílik a fájl. Ha a beszélgetés korábban még nem felfedve (nem látható benne a kapcsolat dekódolt nyilvános neve), ezzel egy időben erre is sor kerül.

A Live Messenger beszélgetéselőzményeinek megjelenítése:

1. A jobb egérgombbal kattintson bármelyik beszélgetésre a Live Messenger Csevegéselőzmény-megjelenítőben, majd válassza a **Megjelenítés** lehetőséget.
2. Ha a rendszer arra kéri, igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.

   A beszélgetés tartalma dekódolva van.

Adott szövegek keresése a beszélgetések szövegében

Szöveget csak a felfedett (dekódolt), a megtekintő ablakában látható beszélgetésekben tud keresni. Ezekben a beszélgetésekben egyszerű szövegként látható a kapcsolat nyilvános neve.

Szövegek keresése a csevegéselőzményekben:

1. Kattintson a **Keresés** gombra a Live Messenger Csevegéselőzmény-megjelenítőben.
2. Írjon be egy keresőkifejezést, állítson be minden kívánt keresési feltételt, majd kattintson az **OK** gombra.

   Az adott szöveget tartalmazó beszélgetések kiemelten látszanak a megtekintő ablakában.

Beszélgetés törlése

1. Válasszon ki egy csevegéselőzményt.
2. Kattintson a **Törlés** gombra.

Oszlopok hozzáadása vagy törlése

Alapértelmezés szerint a Live Messenger Csevegéselőzmény-megjelenítőben mindig a 3 leggyakrabban használt oszlop látható. Ön hozzáadhat és törölhet is oszlopokat a képernyőn láthatóak közül.

Oszlopok hozzáadása a képernyőhöz:

1. Kattintson bármelyik oszlop fejlécére, majd válassza az **Oszlopok hozzáadása vagy törlése** lehetőséget.
2. A bal ablaktáblán válassza ki valamelyik oszlopfejlécet, majd a jobb ablaktáblába helyezéshez kattintson a **Hozzáadás** parancsra.

Oszlopok törlése a képernyőről:

1. Kattintson bármelyik oszlop fejlécére, majd válassza az **Oszlopok hozzáadása vagy törlése** lehetőséget.
2. A jobb ablaktáblán válassza ki valamelyik oszlopfejlécet, majd a bal ablaktáblába helyezéshez kattintson a **Törlés** parancsra.

A megjelenített beszélgetések szűrése

A Live Messenger Csevegéselőzmény-megjelenítőben megjelenik az Ön összes fiókjához tartozó beszélgetések listája. A megjelenített beszélgetéseket az alábbiak szerint is szűrheti:

- Egyes fiókok. További információ: Egy adott fiókhoz tartozó beszélgetések megjelenítése, 65. oldal.
- Időtartam. További információ: Beszélgetések megjelenítése időtartam szerint, 65. oldal.
- Különböző mappák. További információ: A nem az alapértelmezett mappába elmentett beszélgetések megjelenítése, 65. oldal.

Egy adott fiókhoz tartozó beszélgetések megjelenítése

- Válasszon ki egy fiókot a **Fiók előzményeinek megjelenítése** menüből a Live Messenger Csevegéselőzmény-megjelenítőben.

Beszélgetések megjelenítése időtartam szerint

1. Kattintson a **Speciális szűrő** ikonra a Live Messenger Csevegéselőzmény-megjelenítőben.

   Megnyílik a Speciális szűrő párbeszédpanel.
2. Jelölje be a **Csak az adott időtartamon belül beszélgetések megjelenítése** felirat melletti négyzetet.
3. Adja meg az évet, hónapot és napot a **From date** (Ettől az időponttól), illetve a **To date** (Eddig az időpontig) mezőkben, majd az időpontok megadásához kattintson a naptár melletti nyílra.
4. Kattintson az **OK** gombra.

A nem az alapértelmezett mappába elmentett beszélgetések megjelenítése

1. Kattintson a **Speciális szűrő** ikonra a Live Messenger Csevegéselőzmény-megjelenítőben.
2. Jelölje be a **Másik előzményfájl-mappa használata** felirat melletti négyzetet.

3. Adja meg a mappa célhelyét, vagy kattintson a **Tallózás** elemre, hogy megkeresse.
4. Kattintson az **OK** gombra.

Speciális feladatok

Privacy Manager tanúsítványok és megbízható kapcsolatok áthelyezése másik számítógépre

Ön biztonságosan más számítógépre telepítheti a Privacy Manager-tanúsítványokat és a Megbízható kapcsolatok listáját, vagy készíthet biztonsági másolatot az adatairól. Ehhez jelszóval védett fájlként készítsen biztonsági másolatot az adatairól. A fájlt hálózati helyre vagy cserélhető adattároló eszközre mentse, aztán pedig állítsa vissza az új számítógépen.

A Privacy Manager-tanúsítványok és a Megbízható kapcsolatok biztonsági mentése

A Privacy Manager-tanúsítványok és a Megbízható kapcsolatok jelszóval védett fájlba történő biztonsági mentéséhez tegye a következőket:

1. Nyissa meg a Privacy Managert, és kattintson a **Migráció** elemre.
2. Kattintson a **Biztonsági mentés** lehetőségre.
3. A Select Data (Adatmegadás) oldalon adja meg a migrációs fájlban is szereplő adatcsoportokat, majd kattintson a **Next** (Tovább) gombra.
4. A Migration File (Migrációs fájl) oldalon adja meg a fájl nevét, vagy kattintson a **Browse** (Tallózás) elemre, hogy célhelyet keressen neki. Végül kattintson a **Next** (Tovább) gombra.
5. Írjon be és erősítsen meg egy jelszót, majd kattintson a **Tovább** gombra.

MEGJEGYZÉS: A jelszót tárolja biztonságos helyen, mivel szüksége lesz rá a migrációs fájl visszaállításához.

6. Igazolja magát a kiválasztott biztonsági bejelentkezési eljárás segítségével.
7. Kattintson a **Finish** (Befejezés) gombra a Migration File Saved (Migrációs fáj elmentve) oldalon.

A Privacy Manager-tanúsítványok és a Megbízható kapcsolatok visszaállítása

A Privacy Manager-tanúsítványok és a Megbízható kapcsolatok egy másik számítógépre történő, a migrációs folyamat miatti, vagy ugyanarra a számítógépre történő visszaállításához tegye a következőket:

1. Nyissa meg a Privacy Managert, és kattintson a **Migráció** elemre.
2. Kattintson a **Visszaállítás** gombra.
3. A Migration File (Migrációs fájl) oldalon kattintson a **Browse** (Tallózás) elemre, hogy megkeresse a fájlt, majd kattintson a **Next** (Tovább) gombra.
4. Adja meg a biztonsági mentési fájl létrehozása során használt jelszót, majd kattintson a **Tovább** elemre.
5. Kattintson a **Finish** (Befejezés) gombra a Migration File (Migrációs fájl) oldalon.

A Privacy Manager alkalmazás központi felügyelete

Lehetséges, hogy a Privacy Manager alkalmazás telepítésére központi telepítéssel került sor, amelyet a rendszergazda szabott testre. Az alábbi funkciók engedélyezett, illetve letiltott állapotban lehetnek:

- **Tanúsítványhasználati szabályok**: lehetséges, hogy Önnek a Comodo által kiadott Privacy Manager-tanúsítványokat kell használnia, de az is lehetséges, hogy más tanúsító hatóság által kiadott digitális tanúsítványok használatára is kap engedélyt.
- **Titkosítási szabályok**: lehetséges, hogy a titkosítási lehetőségek külön-külön engedélyezett vagy letiltott állapotban vannak a Microsoft Office-ban és az Outlookban, valamint a Windows Live Messenger alkalmazásban.

10 File Sanitizer for HP ProtectTools

A Fájlürítő egy olyan alkalmazás, amellyel biztonságosan szétfoszlathatja bizalmas adatait (személyes fájlok, előzmények, webes adatok vagy más adatkomponensek) a számítógépen, és adott időközönként megtisztíthatja a merevlemezt.

MEGJEGYZÉS: A Fájlürítő alkalmazás jelen verziója csak a rendszerben lévő merevlemezen fut.

Szétfoszlatás

A szétfoszlatás más, mint a szabványos Windows® törlés (a Fájlürítő alkalmazásban „egyszerű törlés”). Amikor a Fájlürítő programban megsemmisít egy fájlt vagy adatot, egy algoritmus először véletlenszerűen felülírja azt, így gyakorlatilag lehetetlenné válik a visszaállítása. Az egyszerű Windows törlés a merevlemezen a fájlt épen vagy olyan állapotban hagyja, amelyből törvényszéki módszerekkel helyreállítható.

Miután kiválaszt egy szétfoszlatásprofilt (Magas biztonság, Közepes biztonság, Alacsony biztonság), egy előkészített lista jelenik meg arról, hogy milyen adatok milyen módszerekkel semmisüljenek meg. A szétfoszlatásprofilt testre szabhatja, így megadhatja, hány menetben történjen az adatok felülírása, milyen adatok kerüljenek a művelet alá, mely adatok igényelnek megerősítést a művelet előtt, és mely adatokat kívánja kivenni a művelet alól. További tudnivalók: Szétfoszlatásprofil kiválasztása vagy létrehozása, 73. oldal.

Beállíthat egy automatikus ütemezést, és kézzel is szétfoszlathatja a fájlokat. További tudnivalók: Szétfoszlatás beütemezése, 72. oldal, Egyes elemek kézi foszlatása, 77. oldal vagy A kiválasztott elemek kézi foszlatása, 77. oldal.

MEGJEGYZÉS: .dll fájlt csak akkor lehet szétfoszlatni és a rendszerből eltávolítani, ha először a lomtárba helyezték.

Szabad hely kifehérítése

Egy fájl vagy adat törlése a Windowsban nem jár a tartalmának eltávolításával a merevlemezről. A Windows csak a hivatkozást törli. A fájlt tartalma azonban továbbra is a merevlemezen marad mindaddig, amíg új adattal felül nem írják ugyanazt a területet a merevlemezen.

A szabad hely kifehérítésével biztonságosan felülírhatja törölt fájljainak tartalmát véletlenszerűen generált adatokkal, így mások nem fognak tudni hozzáférni az eredeti tartalomhoz.

MEGJEGYZÉS: A szabad hely kifehérítése azon fájlokhoz használatos, amelyeket a Windows Lomtárba helyezett, illetve amelyeket kézzel törölt. A szabad hely kifehérítése nem jár további biztonsággal a szétfoszlatott fájlokra nézve.

Automatikus ütemezést is beállíthat a szabad hely kifehérítéséhez, vagy kézzel is elindíthatja, ha a **HP ProtectTools** ikonra kattint az értesítési területen a tálca jobb szélén. További tudnivalók: Ütemezett időpont beállítása a szabad hely kifehérítéséhez, 73. oldal vagy A szabad hely kifehérítésének kézi aktiválása, 78. oldal.

Beállítási eljárások

A Fájlürítő megnyitása

A Fájlürítő megnyitása:

1. Kattintson a **Start**, a **Minden program**, a **HP**, majd a **HP ProtectTools Security Manager** lehetőségre.
2. Kattintson a **Fájlürítő** elemre.

– vagy –

▲ Kattintson duplán a **Fájlürítő** ikonra az asztalon.

– vagy –

▲ A jobb egérgombbal kattintson a tálca jobb szélén látható **HP ProtectTools** ikonra az értesítési területen, kattintson a **Fájlürítő** elemre, majd **A Fájlürítő megnyitása** pontra.

Szétfoszlatás beütemezése

MEGJEGYZÉS: Az előre beállított foszlatásprofilok használatához és létrehozásához lásd: Szétfoszlatásprofil kiválasztása vagy létrehozása, 73. oldal.

MEGJEGYZÉS: Fájlok kézi foszlatásához lásd: Egyes elemek kézi foszlatása, 77. oldal.

1. Nyissa meg a Fájlürítőt, és kattintson a **Foszlatás** lehetőségre.
2. Válasszon foszlatási lehetőséget:
   - **A Windows leállítása**: ezt a lehetőséget akkor válassza, ha a Windows leállításakor minden kiválasztott fájlt szét szeretne foszlatni.

     MEGJEGYZÉS: Ha ezt a beállítást választja, kikapcsoláskor megjelenik egy párbeszédpanel, amely rákérdez, hogy kívánja-e szétfoszlatni a kiválasztott erőforrásokat, vagy inkább mellőzi az eljárást. A foszlatás mellőzéséhez kattintson az **Igen**, a foszlatás végrehajtásához pedig a **Nem** elemre.
   - **Böngésző megnyitásakor**: ezt a lehetőséget akkor válassza, ha az összes webbel kapcsolatos adatot (pl. URL-előzmények) szét szeretné foszlatni, amikor megnyit egy böngészőt.
   - **Böngésző bezárásakor**: ezt a lehetőséget akkor válassza, ha az összes webbel kapcsolatos adatot (pl. URL-előzmények) szét szeretné foszlatni, amikor bezár egy böngészőt.
   - **Billentyűsorrend**: ezt a lehetőséget akkor válassza, ha a szétfoszlatást billentyűsorrenddel kívánja aktiválni.
   - **Ütemező**: jelölje be az **Aktív ütemező** négyzetet, írja be Windows-jelszavát, majd adja meg az időpontot, amikor a szétfoszlatást el szeretné indítani.

   MEGJEGYZÉS: .dll fájlt csak akkor lehet szétfoszlatni és a rendszerből eltávolítani, ha először a lomtárba helyezték.
3. Kattintson az **Alkalmaz**, majd az **OK** gombra.

Ütemezett időpont beállítása a szabad hely kifehérítéséhez

MEGJEGYZÉS: A szabad hely kifehérítése azokra a fájlokra vonatkozik, amelyeket a Windows Lomtár segítségével kézzel törölt. A szabad hely kifehérítése nem jár további biztonsággal a szétfoszlatott fájlokra nézve.

Ütemezett időpont beállítása a szabad hely kifehérítéséhez:

1. Nyissa meg a Fájlürítőt, és kattintson a **Szabad hely kifehérítése** lehetőségre.
2. Jelölje be az **Aktív ütemező** négyzetet, írja be Windows-jelszavát, majd adjon meg egy időpontot, amikor a merevlemezt ki szeretné kifehéríteni.
3. Kattintson az **Alkalmaz**, majd az **OK** gombra.

MEGJEGYZÉS: A szabad hely kifehérítése sok időt vehet igénybe. Bár a szabad hely kifehérítése a háttérben fut, a számítógép teljesítménye a processzorhasználat miatt csökkenhet.

Szétfoszlatásprofil kiválasztása vagy létrehozása

Előre összeállított profil kiválasztásával vagy testre szabott profil létrehozásával megadhatja, hogyan és mely fájlokat szeretne szétfoszlatni.

Előre összeállított foszlatási profil

Amikor előre összeállított foszlatási profilt választ (Magas biztonság, Közepes biztonság vagy Alacsony biztonság), egy előre megadott törlési módozat és bizonyos fájlok listája automatikusan kiválasztásra kerül. Kattintson a **Részletek megtekintése** gombra, hogy megtekintse a foszlatandó fájlok listáját.

Előre összeállított foszlatási profil kiválasztása:

1. Nyissa meg a Fájlürítőt, és kattintson a **Beállítások** lehetőségre.
2. Kattintson az előre összeállított szétfoszlatásprofilra.
3. Kattintson a **Részletek megtekintése** pontra, hogy lássa a foszlatásra kijelölt fájlokat.
4. **A következők szétfoszlatása** alatt jelölje meg azon fájlok négyzeteit, amelyek esetén megerősítést kér a foszlatás előtt.
5. Kattintson az **Alkalmaz**, majd az **OK** gombra.

A foszlatási profil testreszabása

Foszlatási profil létrehozásakor megadhatja a foszlatási ciklusok számát, azt, hogy mely fájlokat szeretné szétfoszlatni, melyek esetén kér megerősítést, valamint hogy mely fájlokat szeretné kivonni a foszlatás alól:

1. Nyissa meg a Fájlürítőt, kattintson a **Beállítások**, a **Speciális biztonsági beállítások**, majd a **Részletek megtekintése** elemre.
2. Adja meg a foszlatási ciklusok számát.

MEGJEGYZÉS: Minden egyes fájl esetén a megadott számú foszlatási ciklus fog lefutni. Ha például 3-at ad meg, a felülírási algoritmus 3-szor egymás után le fog futni. Ha magasabb biztonsági szintű foszlatási ciklust ad meg, a foszlatás időtartama jelentősen megnyúlhat; minél magasabb azonban a megadott foszlatási ciklusok száma, annál kevésbé valószínű, hogy az adatokat be lehet olvasni.

3. Válassza ki a foszlatandó fájlokat:

   a. Az **Elérhető foszlatási lehetőségek** alatt kattintson egy fájlra, majd kattintson a **Hozzáadás** lehetőségre.

   b. Egyéni fájl hozzáadásához kattintson az **Egyéni lehetőség hozzáadása** elemre, majd tallózzon a kérdésre fájlra vagy mappára, vagy írja be az elérési útvonalát. Kattintson a **Megnyitás**, majd az **OK** gombra. Az **Elérhető foszlatási lehetőségek** alatt kattintson az egyéni fájlra, majd a **Hozzáadás** lehetőségre.

MEGJEGYZÉS: Ha törölni kíván egy erőforrást az elérhető foszlatási lehetőségek közül, kattintson rá, majd a **Törlés** gombra.

4. **A következők szétfoszlatása** alatt jelölje meg azon fájlok jelölőnégyzeteit, amelyek esetén megerősítést kér a foszlatás előtt.

MEGJEGYZÉS: Ha törölni kíván egy fájlt az elérhető foszlatási listáról, kattintson rá, majd a **Törlés** gombra.

5. Ha nem szeretné, hogy egyes fájlok vagy mappák automatikusan foszlatásra kerüljenek, kattintson a **Hozzáadás** elemre a **Ne foszlassa a következőket:** alatt, majd keressen rá egy fájl vagy mappa nevére, vagy adja meg. Kattintson a **Megnyitás**, majd az **OK** gombra.

MEGJEGYZÉS: Ha törölni kíván egy fájlt a kivételek listájáról, kattintson rá, majd a **Törlés** gombra.

6. Ha végzett a szétfoszlatásprofil beállításával, kattintson az **Alkalmaz**, majd az **OK** gombra.

Egyszerű törlési profil testreszabása

Az egyszerű törlési profil sima törlést hajt végre, foszlatás nélkül. Egyszerű törlési profil testreszabásánál megadhatja, mely fájlokat szeretne törölni, melyek igényelnek megerősítést törlés előtt, valamint hogy mely fájlokat szeretné felvenni a kivételek közé.

MEGJEGYZÉS: Ha az egyszerű törlést használja, a szabad hely alkalmankénti kifehérítésére a kézzel törölt vagy a Windows Lomtárba helyezett erőforrásokból kerülhet sor.

Egyszerű törlési profil testreszabása:

1. Nyissa meg a Fájlürítőt, kattintson a **Beállítások**, a **Speciális biztonsági beállítások**, majd a **Részletek megtekintése** lehetőségre.

2. Válassza ki a törlendő fájlokat:

   a. Az **Elérhető törlési lehetőségek** alatt kattintson egy fájlra, majd kattintson a **Hozzáadás** lehetőségre.

   b. Egyéni fájl hozzáadásához kattintson az **Egyéni lehetőség hozzáadása** elemre, adja meg a fájl vagy mappa nevét, majd kattintson az **OK** gombra. Kattintással jelölje meg a kérdéses fájlt, majd kattintson a **Hozzáadás** gombra.

MEGJEGYZÉS: Ha törölni kíván egy fájlt az elérhető törlési lehetőségek közül, kattintson rá, majd a **Törlés** gombra.

3. **A következők törlése** lehetőség alatt jelölje be az azon fájlok melletti négyzeteket, amelyekhez megerősítést kér a törlés előtt.

MEGJEGYZÉS: Ha törölni kíván egy fájlt az elérhető törlési listáról, kattintson rá, majd a **Törlés** gombra.

4. A **Ne törölje a következőket** lehetőség alatt kattintson a **Hozzáadás** gombra, hogy megadhassa, mely fájlokat szeretné kivonni a törlés alól.

MEGJEGYZÉS: Ha törölni kíván egy fájlt a kivételek listájáról, kattintson rá, majd a **Törlés** gombra.

5. Ha végzett az egyszerű törlési profil beállításával, kattintson az **Alkalmaz**, majd az **OK** gombra.

Általános feladatok

A Fájlürítőt a következő feladatok ellátására használhatja:

- Billentyűkombináció a szétfoszlatáshoz: ezzel a lehetőséggel saját billentyűkombinációhoz (például ctrl+alt+s) rendelheti a foszlatási művelet megkezdését. További információ: Billentyűkombináció használata a szétfoszlatás megkezdéséhez, 76. oldal.
- Fájlürítő ikon a szétfoszlatáshoz: ez a lehetőség a Windows egéráthúzásos módszeréhez hasonlóan működik. További információ: A Fájlürítő ikon használata, 77. oldal.
- Egyes elemek vagy minden kiválasztott elem kézi foszlatása: kézzel is szétfoszlathat fájlokat, így nem kell az ütemezett foszlatásra várnia. További információ: Egyes elemek kézi foszlatása, 77. oldal vagy A kiválasztott elemek kézi foszlatása, 77. oldal.
- A szabad hely kifehérítésének kézi aktiválása: kézzel aktiválja a szabad hely kifehérítését. További információ: A szabad hely kifehérítésének kézi aktiválása, 78. oldal.
- A szétfoszlatás vagy a szabad hely kifehérítésének leállítása: leállíthat egy folyamatban lévő foszlatást vagy szabad hely kifehérítésének műveletét. További információ: A szétfoszlatás vagy a szabad hely kifehérítésének leállítása, 78. oldal.
- A naplófájlok megtekintése: megtekinthetők a foszlatás és a szabad hely kifehérítésének naplófájljai, amelyekbe az utolsó műveletben történt hibák vannak feljegyezve. További információ: A naplófájlok megtekintése, 78. oldal.

MEGJEGYZÉS: A foszlatás vagy a szabad hely kifehérítése hosszú időt vehet igénybe. Bár a foszlatás és a szabad hely kifehérítése a háttérben fut, a számítógép teljesítménye csökkenhet a processzorhasználat miatt.

Billentyűkombináció használata a szétfoszlatás megkezdéséhez

Billentyűkombináció az alábbi lépésekkel állítható be:

1. Nyissa meg a Fájlürítőt, és kattintson a **Foszlatás** lehetőségre.
2. Jelölje be a **Billentyűkombináció** négyzetet.
3. Adjon meg egy karaktert a szövegmezőben.
4. Jelölje be vagy a **CTRL**, vagy az **ALT** melletti négyzetet, majd válassza a **SHIFT** mezőt.

   Például, ha az automatikus foszlatást az s billentyű és a ctrl+shift kombinációjával szeretné elindítani, írja az s karaktert a mezőbe, majd jelölje be a **CTRL** és a **SHIFT** melletti négyzetet.

MEGJEGYZÉS: Ügyeljen rá, hogy ne válasszon olyan billentyűkombinációt, amit már használ.

Billentyűkombináció használata a foszlatás megkezdéséhez:

1. A kiválasztott karakter leütése közben tartsa lenyomva a shift és a ctrl vagy az alt billentyűt (vagy az Ön által megadott billentyűkombinációt).
2. A megerősítést kérő párbeszédpanel megnyílása után kattintson az **Igen** gombra.

A Fájlürítő ikon használata

△ **VIGYÁZAT!** Szétfoszlatott fájlokat nem lehet helyreállítani. Legyen elővigyázatos, amikor a kézi foszlatásnál kiválasztja az elemeket.

1. Tallózzon arra a dokumentumra vagy mappára, amelyet szét szeretne foszlatni.
2. Húzza a fájlt a **File Sanitizer** (Fájlürítő) ikonra az asztalon.
3. A megerősítést kérő párbeszédpanel megnyílása után kattintson az **Igen** gombra.

Egyes elemek kézi foszlatása

△ **VIGYÁZAT!** Szétfoszlatott fájlokat nem lehet helyreállítani. Legyen elővigyázatos, amikor a kézi foszlatásnál kiválasztja az elemeket.

1. A jobb egérgombbal kattintson a tálca jobb oldalán található értesítési területen látható **HP ProtectTools** ikonra, válassza a **Fájlürítő** lehetőséget, majd pedig az **Egy elem szétfoszlatása** elemet.
2. A Tallózó párbeszédpanel megnyitása után tallózzon a foszlatni kívánt elemre, majd kattintson az **OK** gombra.

MEGJEGYZÉS: A foszlatandó elem fájl vagy mappa is lehet.

3. A megerősítést kérő párbeszédpanel megnyílása után kattintson az **Igen** gombra.

– vagy –

1. A jobb egérgombbal kattintson a **Fájlürítő** ikonra az asztalon, majd kattintson az **Egy elem szétfoszlatása** lehetőségre.
2. A Tallózó párbeszédpanel megnyitása után tallózzon a foszlatni kívánt elemre, majd kattintson az **OK** gombra.
3. A megerősítést kérő párbeszédpanel megnyílása után kattintson az **Igen** gombra.

– vagy –

1. Nyissa meg a Fájlürítőt, és kattintson a **Foszlatás** lehetőségre.
2. Kattintson a **Tallóz** gombra.
3. A Tallózó párbeszédpanel megnyitása után tallózzon a foszlatni kívánt elemre, majd kattintson az **OK** gombra.
4. A megerősítést kérő párbeszédpanel megnyílása után kattintson az **Igen** gombra.

A kiválasztott elemek kézi foszlatása

1. A jobb egérgombbal kattintson a tálca jobb oldalán található értesítési területen látható **HP ProtectTools** ikonra, válassza a **Fájlürítő** lehetőséget, majd pedig a **Foszlatás most** elemet.
2. A megerősítést kérő párbeszédpanel megnyílása után kattintson az **Igen** gombra.

– vagy –

1. A jobb egérgombbal kattintson a **Fájlürítő** ikonra az asztalon, majd kattintson az **Foszlatás most** lehetőségre.
2. A megerősítést kérő párbeszédpanel megnyílása után kattintson az **Igen** gombra.

– vagy –

1. Nyissa meg a Fájlürítőt, és kattintson a **Foszlatás** lehetőségre.
2. Kattintson a **Foszlatás most** gombra.
3. A megerősítést kérő párbeszédpanel megnyílása után kattintson az **Igen** gombra.

A szabad hely kifehérítésének kézi aktiválása

1. A jobb egérgombbal kattintson a tálca jobb oldalán található értesítési területen látható **HP ProtectTools** ikonra, válassza a **Fájlürítő** lehetőséget, majd pedig a **Fehérítés most** elemet.
2. A megerősítést kérő párbeszédpanel megnyílása után kattintson az **Igen** gombra.

– vagy –

1. Nyissa meg a Fájlürítőt, és kattintson a **Szabad hely kifehérítése** lehetőségre.
2. Kattintson a **Fehérítés most** elemre.
3. A megerősítést kérő párbeszédpanel megnyílása után kattintson az **Igen** gombra.

A szétfoszlatás vagy a szabad hely kifehérítésének leállítása

Amikor egy foszlatási vagy kifehérítési művelet folyamatban van, egy üzenet jelenik meg a HP ProtectTools Security Manager ikonja felett az értesítési területen. Az üzenet tájékoztatja a foszlatási vagy kifehérítési művelet részleteiről (százalékos teljesítettség), és lehetőséget ad annak megszakítására is.

A művelet megszakítása:

▲ A művelet megszakításához kattintson az üzenetre, majd a **Leállítás** gombra.

A naplófájlok megtekintése

Minden foszlatási vagy kifehérítési művelet végrehajtásakor létrejön egy. a felmerülő hibákat tartalmazó naplófájl. A naplófájlok mindig a legutolsó foszlatási vagy kifehérítési művelet adatait tartalmazzák.

MEGJEGYZÉS: A sikeresen szétfoszlatott vagy kifehérített fájlok nem jelennek meg a naplófájlban.

Külön naplófájlok készülnek a foszlatási és a kifehérítési műveletekről. Mindkét naplófájl a következő helyen található meg:

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

11 Device Access Manager for HP ProtectTools (csak egyes típusokon)

A Windows® operációs rendszer adminisztrátorai használják az Eszközkezelőt, hogy beállítsák, a rendszeren mely eszközökhöz férhet hozzá a HP ProtectTools, és mely eszközöket kíván levédeni az illetéktelen hozzáférés ellen:

- A felhasználók számára létrehozott eszközprofilok meghatározzák, mely eszközökhöz férnek, illetve nem férnek hozzá.
- A felhasználók ezenkívül csoportokba tartoznak, ami lehet az előre megadott Eszközadminisztrátor csoport, vagy a Vezérlőpult Felügyeleti eszközök részének Számítógép-kezelés szolgáltatásával létrehozott egyéb felhasználói csoport.
- Az eszközhozzáférés csoporttagság alapján engedélyezhető vagy tiltható le.
- Az olyan eszközosztályokhoz, mint a CD-ROM- és a DVD-meghajtók, az olvasási és írási hozzáférés külön szabályozható.

Korlátozott felhasználóknak is engedélyt lehet adni arra, hogy olvassák és módosítsák az eszközhozzáférés házirendjét.

Beállítási eljárások

Az Eszközkezelő megnyitása

Az Eszközkezelő megnyitásához kövesse az alábbi lépéseket:

1. Kattintson a **Start**, a **Minden program**, a **HP**, majd a **HP ProtectTools Administrative Console** elemre.
2. A bal oldali ablaktáblán kattintson az **Eszközkezelő** elemre.

Az eszközhozzáférés beállítása

Az Eszközkezelő a HP ProtectTools alkalmazáshoz a következő három nézetet ajánlja fel:

- Az Egyszerű beállítások nézet az Eszköz rendszergazdái csoport tagjainak eszközosztályaihoz enged tiltási vagy engedélyezési beállítást.
- Az Eszközosztály beállításai nézet adott felhasználók vagy csoportok adott eszközeihez vagy eszköztípusaihoz enged tiltási vagy engedélyezési beállítást.
- A Felhasználók hozzáférése beállítás nézetben megadható, mely felhasználók láthatják vagy módosíthatják az Egyszerű beállítások és Eszközosztály beállításai nézet elemeit.

Eszköz rendszergazdái csoport

Az Eszközkezelő telepítésekor egy Eszköz rendszergazdái csoport kerül létrehozásra.

A rendszergazda egy adott eszközosztályhoz való hozzáférés megtagadásával egyszerű eszköz-hozzáférési felügyeleti szabályt vezethet be, hacsak a felhasználó nem minősül megbízhatónak (az eszközhozzáférés tekintetében). Az eszközhasználat szempontjából megbízható és az eszközhasználat szempontjából nem megbízható felhasználók megkülönböztetéséhez azt javasoljuk, hogy az eszközhasználat szempontjából megbízható összes felhasználót vegye fel az Eszköz rendszergazdái csoportba. Az, hogy az Eszköz rendszergazdái csoport tagjai az Egyszerű konfiguráció vagy az Eszközosztály-konfiguráció nézeten keresztül hozzáférhetnek az eszközökhöz, egyúttal azt is biztosítja, hogy az eszközhasználat szempontjából megbízható felhasználók teljes hozzáférést kapnak az adott eszközosztályokhoz.

MEGJEGYZÉS: Egy felhasználónak az Eszköz rendszergazdái csoporthoz való hozzáadása nem jelenti automatikusan azt, hogy a felhasználónak hozzáférése lesz az eszközökhöz. Ugyanakkor használhatja az Egyszerű beállítások nézetet, hogy hozzáféréseket adjon bizonyos eszközosztályokhoz a megbízható felhasználók számára.

Felhasználóknak az Eszköz rendszergazdái csoporthoz való hozzáadásához kövesse az alábbi lépéseket:

- Windows 7, Vista vagy XP Professional rendszerekben használja a Vezérlőpult szabványos „Helyi felhasználók és csoportok” beépülőjét.
- Windows 7, Vista vagy XP Home rendszerekben egy erre jogosult felhasználói fiókban írja a következőt a parancssorba:

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

Egyszerű beállítások

Rendszergazdák és jogosult felhasználók használhatják az Egyszerű beállítások nézetet, hogy módosítsák a hozzáférést a következő eszközosztályokhoz az összes nem eszközrendszergazda számára:

MEGJEGYZÉS: Ahhoz, hogy ezt a nézetet használja az eszköz-hozzáférési információk kiolvasásához, a felhasználónak vagy csoportnak olvasási hozzáféréssel kell rendelkeznie a **Felhasználói hozzáférések kezelése** nézetben. Ahhoz, hogy ezt a nézetet használja az eszköz-hozzáférési információk módosításához, a felhasználónak vagy csoportnak módosítási hozzáféréssel kell rendelkeznie a **Felhasználói hozzáférések kezelése** nézetben.

- Az összes cserélhető adathordozó (lemezek, pendrive-ok stb.)
- Az összes DVD/CD-ROM-meghajtó
- Az összes soros és párhuzamos port
- Az összes Bluetooth®-eszköz
- Az összes infravörös eszköz
- Az összes modemeszköz
- Az összes PCMCIA-eszköz
- Az összes 1394-es szabványú eszköz

Egy eszközosztályhoz való hozzáférés engedélyezése vagy letiltása az összes, nem az Eszköz rendszergazdái csoportba tartozó rendszergazda számára:

1. A **HP ProtectTools Administrative Console** bal oldalán kattintson az **Eszközkezelő**, majd az **Egyszerű beállítások** elemre.
2. A hozzáférés megtagadásához jelölje be az adott eszközosztály vagy eszköz melletti négyzetet a jobb ablaktáblán. Vegye ki a jelölést a négyzetből, ha engedélyezni kívánja a hozzáférést.

   Ha a jelölőnégyzet szürke, a hozzáférési értékek módosítva lettek az Eszközosztály beállításai nézetben. Az értékek egyszerű beállításokra történő visszaállításához jelölje be a hozzá tartozó négyzetet, vagy a beállításhoz törölje a jelölést a négyzetből, majd kattintson az **Igen** gombra a megerősítéshez.
3. Kattintson a **Mentés** ikonra.

   MEGJEGYZÉS: Ha nem fut a háttérszolgáltatás, egy párbeszédpanel jelenik meg, amely felajánlja az elindítását. Kattintson az **Igen** gombra.
4. Kattintson az **OK** gombra.

Háttérszolgáltatás indítása

Az eszközprofilok alkalmazása előtt a HP ProtectTools Security Manager megnyit egy párbeszédpanelt, hogy megkérdezze, el szeretné-e indítani a HP ProtectTools Device Locking/Auditing háttérszolgáltatást. Kattintson az **Igen** gombra. A háttérszolgáltatás elindul, és ezentúl minden rendszerindításkor bekapcsol.

MEGJEGYZÉS: Egy eszközprofilt meg kell adni, mielőtt a háttérszolgáltatást felajánló ablak megjelenik.

A szolgáltatást rendszergazdák is leállíthatják és elindíthatják:

1. Kattintson a **Start** gombra, majd a **Vezérlőpanel** parancsra.
2. Kattintson a **Felügyeleti eszközök** elemre, majd a **Szolgáltatások** lehetőségre.
3. Keresse meg a **HP ProtectTools Device Locking/Auditing** szolgáltatást.

Az eszközzároló/-figyelő szolgáltatás leállítása nem szünteti meg az eszköz zárolását. Az eszközzárolást két összetevő biztosítja:

- Device Locking/Auditing szolgáltatás
- DAMDrv.sys meghajtó

A szolgáltatás elindítása elindítja az eszközmeghajtót, de a szolgáltatás leállítása nem állítja le a meghajtót.

A háttérszolgáltatás futásának ellenőrzéséhez nyissa meg a parancssort, és írja be: sc query flcdlock.

Az eszközmeghajtó futásának ellenőrzéséhez nyissa meg a parancssort, és írja be: sc query damdrv.

Eszközosztály beállításai

Rendszergazdák és jogosult felhasználók megtekinthetik és módosíthatják a felhasználók és csoportok azon listáját, amelyek engedélyezve vagy tiltva vannak eszközökhöz vagy eszközosztályokhoz.

MEGJEGYZÉS: Ahhoz, hogy ezt a nézetet használja az eszköz-hozzáférési információk kiolvasásához, a felhasználónak vagy csoportnak olvasási hozzáféréssel kell rendelkeznie a **Felhasználói hozzáférések kezelése** nézetben. Ahhoz, hogy ezt a nézetet használja az eszköz-hozzáférési információk módosításához, a felhasználónak vagy csoportnak módosítási hozzáféréssel kell rendelkeznie a **Felhasználói hozzáférések kezelése** nézetben.

Az Eszközosztály beállításai nézet az alábbi részekből áll:

- **Eszközlista**: azok az eszközosztályok és eszközök, amelyek a rendszeren telepítve vannak vagy előzőleg voltak.
  - Védelmet általában eszközosztályra alkalmaznak. Egy kijelölt felhasználó vagy csoport majd' bármilyen eszközhöz és eszközcsoporthoz hozzáférhet.
  - Védelmet adott eszközre is lehet alkalmazni.
- **Felhasználói lista**: azon felhasználók és csoportok, amelyekhez engedélyezve vagy tiltva van a kijelölt eszközosztályokhoz vagy eszközökhöz való hozzáférés.
  - A Felhasználói listán egy bejegyzés lehet adott felhasználó, illetőleg egy csoport, amelynek a felhasználó is tagja.
  - Ha egy, a Felhasználói listán lévő felhasználó vagy csoport nem áll rendelkezésre, a beállítás az Eszközlistán vagy az Osztály mappában lévő eszközosztályból van származtatva.
  - Az egyes eszközosztályokhoz, például a DVD-hez vagy CD-ROM-hoz való hozzáférés külön az olvasás és külön az írás hozzáférésének beállításával tovább szabályozható.

    Más eszközök és osztályok esetén az olvasási és írási jogokat származtatni lehet. Például az írási jogokat egy magasabb szintű osztályból lehet származtatni, de az írási jogok külön is megvonhatók egy felhasználótól vagy csoporttól.

MEGJEGYZÉS: Ha az Olvasás jelölőnégyzet üres, a hozzáférési bejegyzés nincs hatással az eszköz olvasási hozzáférésére. Nem biztosítja és nem vonja meg az eszközhöz való olvasási hozzáférést.

1. példa: ha egy felhasználó vagy csoport írási hozzáférése meg van tagadva egy adott eszközhöz vagy eszközosztályhoz:

Ugyanaz a felhasználó vagy csoport, ill. csoporttag csak az eszközhierarchiában az eszköz alatti eszközökre kaphat engedélyt írásra vagy olvasásra+írásra.

2. példa: ha egy felhasználó vagy csoport írási hozzáférése engedélyezve van egy adott eszközhöz vagy eszközosztályhoz:

Ugyanannak a felhasználónak vagy csoportnak, ill. csoporttagnak csak az eszközhierarchiában az eszköz alatti eszközökre tilthatók meg a hozzáférési jogai írásra vagy olvasásra+írásra.

3. példa: ha egy felhasználó vagy csoport olvasásra való hozzáférése engedélyezve van egy adott eszközhöz vagy eszközosztályhoz:

Ugyanannak a felhasználónak vagy csoportnak, ill. csoporttagnak csak az eszközhierarchiában az eszköz alatti eszközökre tilthatók meg a hozzáférési jogai olvasásra vagy olvasásra+írásra.

4. példa: ha egy felhasználó vagy csoport olvasásra való hozzáférése tiltva van egy adott eszközhöz vagy eszközosztályhoz:

Ugyanaz a felhasználó vagy csoport, ill. csoport tagja csak az eszközhierarchiában az eszköz alatti eszközökre kaphat engedélyt olvasásra vagy olvasásra+írásra.

5. példa: ha egy felhasználó vagy csoport olvasásra+írásra való hozzáférése engedélyezve van egy adott eszközhöz vagy eszközosztályhoz:

Ugyanannak a felhasználónak vagy csoportnak, ill. csoporttagnak csak az eszközhierarchiában az eszköz alatti eszközökre tilthatók meg a hozzáférési jogai írásra vagy olvasásra+írásra.

6. példa: ha egy felhasználó vagy csoport olvasásra+írásra való hozzáférése tiltva van egy adott eszközhöz vagy eszközosztályhoz:

Ugyanaz a felhasználó vagy csoport, ill. csoporttag csak az eszközhierarchiában az eszköz alatti eszközökre kaphat engedélyt olvasásra vagy olvasásra+írásra.

Hozzáférés megtagadása egy felhasználótól vagy csoporttól

Felhasználónak vagy csoportnak egy eszközhöz vagy eszközosztályhoz való hozzáférésének megelőzése:

1. A **HP ProtectTools Administrative Console** bal oldalán kattintson az **Eszközkezelő**, majd az **Eszközosztály beállításai** elemre.
2. Az eszközlistában kattintson a konfigurálni kívánt eszközosztályra.
   - Eszközosztály
   - Minden eszköz
   - Egyes eszközök

3. A **Felhasználó/csoportok** részben kattintson arra a felhasználóra vagy csoportra, akiktől meg kívánja tagadni a hozzáférést.
4. Kattintson a **Megtagadás** feliratra a felhasználó vagy csoport mellett.
5. Kattintson a **Mentés** ikonra.

MEGJEGYZÉS: Ha az engedélyezés vagy megtagadás a felhasználóval egyező eszközszinten van beállítva, a hozzáférési beállítás elsőbbséget élvez az engedélyezési hozzáférések előtt.

Hozzáférés engedélyezése felhasználó vagy csoport számára

Felhasználónak vagy csoportnak egy eszközhöz vagy eszközosztályhoz való hozzáférésének engedélyezése:

1. A **HP ProtectTools Administrative Console** bal oldalán kattintson az **Eszközkezelő**, majd az **Eszközosztály beállításai** elemre.
2. Az eszközlistán kattintson a következők egyikére:
   - Eszközosztály
   - Minden eszköz
   - Egyes eszközök
3. Kattintson a **Hozzáadás** gombra.

   Megjelenik a **Felhasználók vagy csoportok kijelölése** párbeszédpanel.
4. Felhasználók és csoportok kereséséhez és hozzáadásához kattintson a **Speciális**, majd a **Keresés most** elemre.
5. Kattintson az engedélyezni kívánt felhasználóra vagy csoportra, majd kattintson az **OK** gombra.
6. Kattintson újra az **OK** gombra.
7. A hozzáférésnek a felhasználó számára történő engedélyezéséhez kattintson az **Engedélyezés** gombra.
8. Kattintson a **Mentés** ikonra.

Hozzáférés eltávolítása felhasználótól vagy csoporttól

Felhasználónak vagy csoportnak egy eszközhöz vagy eszközosztályhoz való hozzáférésének eltávolítása:

1. A **HP ProtectTools Administrative Console** bal oldalán kattintson az **Eszközkezelő**, majd az **Eszközosztály beállításai** elemre.
2. Az eszközlistában kattintson a konfigurálni kívánt eszközosztályra.
   - Eszközosztály
   - Minden eszköz
   - Egyes eszközök

3. A **Felhasználó/csoportok** alatt kattintson az eltávolítani kívánt felhasználóra vagy csoportra, majd kattintson az **Eltávolítás** gombra.

4. Kattintson a **Mentés** ikonra.

Egy eszközosztályhoz való hozzáférés engedélyezése egy felhasználó vagy csoport számára

Felhasználó hozzáférésének engedélyezése egy eszközosztályhoz úgy, hogy a felhasználó csoportjának többi tagjának hozzáférése meg legyen tagadva:

1. A **HP ProtectTools Administrative Console** bal oldalán kattintson az **Eszközkezelő**, majd az **Eszközosztály beállításai** elemre.

2. Az eszközlistában kattintson a konfigurálni kívánt eszközosztályra.

   - Eszközosztály
   - Minden eszköz
   - Egyes eszközök

3. A **Felhasználó/csoportok** részben jelölje ki azt a csoportot, amelytől meg kívánja tagadni a hozzáférést, majd kattintson a **Megtagadás** gombra.

4. Lépjen lent a kívánt osztály mappájára, és vegye fel az adott felhasználót.

5. A hozzáférés felhasználó számára történő engedélyezéséhez kattintson az **Engedélyezés** gombra.

6. Kattintson a **Mentés** ikonra.

Egy adott eszközhöz való hozzáférés engedélyezése egy felhasználó vagy csoport számára

Rendszergazdák engedélyezhetik egy felhasználónak egy adott eszközhöz való hozzáférését úgy, hogy a felhasználó csoportjának többi tagja nem férhet az osztály eszközeihez.

1. A **HP ProtectTools Administrative Console** bal oldalán kattintson az **Eszközkezelő**, majd az **Eszközosztály beállításai** elemre.

2. Az eszközlistában kattintson a konfigurálni kívánt eszközosztályra, majd lépjen az alatta lévő mappára.

3. Kattintson a **Hozzáadás** gombra. Megjelenik a **Felhasználók vagy csoportok kijelölése** párbeszédpanel.

4. Kattintson a **Speciális**, majd a **Keresés** elemre, hogy megkeresse azt a csoportot, amelytől meg kívánja tagadni a hozzáférést az eszközökhöz.

5. Kattintson a csoportra, majd az **OK** gombra.

6. Tallózzon az eszközosztály azon eszközére, amelyhez hozzáférést szeretne adni a felhasználó számára.

7. Kattintson a **Hozzáadás** gombra. Megjelenik a **Felhasználók vagy csoportok kijelölése** párbeszédpanel.

8. Felhasználók és csoportok kereséséhez és hozzáadásához kattintson a **Speciális**, majd a **Keresés most** elemre.

9. Kattintson arra a felhasználóra, akinek engedélyezni kívánja a hozzáférést, majd kattintson az **OK** gombra.

10. A hozzáférés felhasználó számára történő engedélyezéséhez kattintson az **Engedélyezés** gombra.

11. Kattintson a **Mentés** ikonra.

Beállítások visszaállítása

△ **VIGYÁZAT!** A beállítások visszaállítása minden eszközkonfigurációs értéket visszaállít a gyári értékre.

A beállítások visszaállítása a gyári értékre:

1. A **HP ProtectTools Administrative Console** bal oldalán kattintson az **Eszközkezelő**, majd az **Eszközosztály beállításai** elemre.

2. Kattintson a **Visszaállítás** gombra.

3. Kattintson az **Igen** gombra a megerősítéshez.

4. Kattintson a **Mentés** ikonra.

Speciális feladatok

A konfigurációs beállításokhoz való hozzáférés szabályozása

A **Felhasználói hozzáférések beállításai** nézetben a rendszergazdák megadják, mely csoportok vagy felhasználók rendelkeznek engedéllyel az Egyszerű beállítások és az Eszközosztály beállításai oldalakhoz.

MEGJEGYZÉS: Egy felhasználónak vagy csoportnak teljes rendszergazdai jogosultságokkal kell rendelkeznie ahhoz, hogy módosítani tudja a felhasználói hozzáférések beállításait.

- Egy felhasználónak vagy csoportnak a Felhasználói hozzáférések beállításaiban a „A konfigurációs beállítások megtekintése (csak olvasásra)” jogosultsággal kell rendelkeznie ahhoz, hogy megtekinthesse az Egyszerű beállítások és az Eszközosztály beállításai információit.
- Egy felhasználónak vagy csoportnak a Felhasználói hozzáférések beállításaiban a „Konfigurációs beállítások módosítása” jogosultsággal kell rendelkeznie ahhoz, hogy módosíthassa az Egyszerű beállítások és az Eszközosztály beállításai információit.

MEGJEGYZÉS: Még a rendszergazdai csoport tagjainak is „olvasási” joggal kell rendelkezniük ahhoz, hogy megtekinthessék az Egyszerű beállítások és az Eszközosztály beállításai nézetet, és „módosítási” joggal ahhoz, hogy ezen nézetek értékeit megváltoztathassák.

MEGJEGYZÉS: Ha a hozzáférési szintek kiértékelése után egy felhasználónak nincs beállítva „Engedélyezés” vagy „Megtagadás” jogosultsága egy adott hozzáférési szinthez, a felhasználó hozzáférése azon a szinten meg lesz tagadva.

Hozzáférés engedélyezése létező csoport vagy felhasználó számára

Engedély megadása létező csoport vagy felhasználó számára a konfigurációs beállítások megtekintéséhez vagy módosításához:

1. A **HP ProtectTools Administrative Console** bal oldalán kattintson az **Eszközkezelő**, majd a **Felhasználói hozzáférések beállításai** elemre.
2. Kattintson egy csoportra vagy felhasználóra az engedély megadásához.
3. Az **Engedélyek** alatt kattintson az **Engedélyezés** pontra minden engedélytípusnál a kijelölt csoportnál vagy felhasználónál:

   MEGJEGYZÉS: Az engedélyek kumulatívak. Például, ha egy felhasználó megkapta a „A konfigurációs beállítások módosítása” engedélyt, ugyanez a felhasználó megkapja a „A konfigurációs beállítások megtekintése (csak olvasás)” engedélyt is. Ha egy felhasználó megkapja a „Teljes rendszergazdai jogokat”, automatikusan megkapja a „A konfigurációs beállítások módosítása” és a „A konfigurációs beállítások megtekintése (csak olvasás)” engedélyt is.

   - Teljes rendszergazdai jogok
   - A konfigurációs beállítások módosítása
   - A konfigurációs beállítások megtekintése (csak olvasás)
4. Kattintson a **Mentés** ikonra.

Hozzáférés megtagadása létező csoport vagy felhasználó számára

Létező csoport vagy felhasználó engedélyének megtagadása a konfigurációs beállítások megtekintéséhez vagy módosításához:

1. A **HP ProtectTools Administrative Console** bal oldalán kattintson az **Eszközkezelő**, majd a **Felhasználói hozzáférések beállításai** elemre.
2. Kattintson egy csoportra vagy felhasználóra az engedély megtagadásához.
3. Az **Engedélyek** alatt kattintson a **Megtagadás** pontra minden engedélytípusnál a kijelölt csoportnál vagy felhasználónál:
   - Teljes rendszergazdai jogok
   - A konfigurációs beállítások módosítása
   - A konfigurációs beállítások megtekintése (csak olvasás)
4. Kattintson a **Mentés** ikonra.

Új csoport vagy felhasználó hozzáadása

Engedély megadása új csoport vagy felhasználó számára a konfigurációs beállítások megtekintéséhez vagy módosításához:

1. A **HP ProtectTools Administrative Console** bal oldalán kattintson az **Eszközkezelő**, majd a **Felhasználói hozzáférések beállításai** elemre.
2. Kattintson a **Hozzáadás** gombra. Megjelenik a **Felhasználók vagy csoportok kijelölése** párbeszédpanel.
3. Felhasználók és csoportok kereséséhez és hozzáadásához kattintson a **Speciális**, majd a **Keresés most** elemre.
4. Kattintson a csoportra vagy felhasználóra, kattintson az **OK** gombra, majd kattintson újra az **OK** gombra.
5. A hozzáférés felhasználó számára történő engedélyezéséhez kattintson az **Engedélyezés** gombra.
6. Kattintson a **Mentés** ikonra.

Csoport vagy felhasználó hozzáférésének eltávolítása

Csoport vagy felhasználó engedélyének eltávolítása a konfigurációs beállítások megtekintéséhez vagy módosításához:

1. A **HP ProtectTools Administrative Console** bal oldalán kattintson az **Eszközkezelő**, majd a **Felhasználói hozzáférések beállításai** elemre.
2. Kattintson egy csoportra vagy felhasználóra, majd kattintson az **Eltávolítás** lehetőségre.
3. Kattintson a **Mentés** ikonra.

Kapcsolódó dokumentum

A Device Access Manager for HP ProtectTools alkalmazás kompatibilis a HP ProtectTools Enterprise Device Access Manager termékkel. A nagyvállalati verzió használatakor a Device Access Manager for HP ProtectTools alkalmazás csak olvasást engedélyez a saját szolgáltatásaiban.

További információk a Device Access Manager for HP ProtectTools alkalmazással kapcsolatban: http://www.hp.com/hps/security/products.

12 LoJack Pro for HP ProtectTools

Az Absolute Software által gyártott Computrace termékek segítségével a felhasználók nyomon tudják követni a számítógépeiket, és tovább növelhetik az adatvédelem erősségét. A Computrace LoJack termékek emellett csökkentik az elromlott gépek számát, és segítenek az elromlott gépek helyreállításában.

A Computrace terméket az alábbi módon tudja aktiválni:

1. Kattintson a **Start**, a **Minden program**, majd a **HP ProtectTools Security Manager** lehetőségre.
2. Kattintson a **Theft Recovery** (Lopás utáni helyreállítás), majd az **Activate Now** (Aktiválás most) parancsra.

   Az alapértelmezett webböngésző megnyitja azt a webhelyet, ahol Ön előfizethet a HP ProtectToolshoz rendelkezésre álló három Computrace termék valamelyikére:

   - **Computrace Data Delete**: távoli adattörlést, eszközlefagyást, illetve alapvető eszközkövetést és -jelentést biztosít.
   - **Computrace LoJack Pro**: távoli adattörlést, eszközlefagyást, alapvető eszközkövetést és -jelentést, illetve lopás utáni helyreállítást biztosít.
   - **Computrace LoJack Pro Premium**: távoli adattörlést, eszközlefagyást, speciális eszközkövetést és -jelentést, földrajzihely-azonosítást és útvonal-letérési riasztást, illetve lopás utáni helyreállítást biztosít.

A Computrace Agent alkalmazás a HP noteszgépek rendszer BIOS-ába van integrálva, bár a számítógép alapállapotában inaktív. Miután előfizetett valamelyik termékre, az Agent aktiválódik. A beágyazott Agent képes az operációs rendszer újratelepítésére és a merevlemezek újraformázására.

MEGJEGYZÉS: Az előfizetési időszak 1–5 év lehet. További részletekért nézze át az Absolute Software tagsági megállapodását. A helyreállítási szolgáltatás a földrajzi helytől függ. A GPS-szel történő nyomon követés csak egyes, WWAN-kompatibilis típusokon támogatott.

13 Hibaelhárítás

HP ProtectTools Security Manager

Rövid leírás	Részletek	Megoldás
Az intelligens kártyák és USB-tokenek nem állnak rendelkezésre a Security Managerben, ha a Security Manager után lettek telepítve.	Annak érdekében, hogy intelligens kártyákat vagy USB-tokeneket használjon a Security Managerben, a támogató szoftvert (illesztőprogramok, PKCS#11 szolgáltatók, stb.) még a Security Manager telepítése előtt telepíteni kell. Ha Önnél már telepítve van a Security Manager, kövesse az alábbi lépéseket az intelligens kártya vagy token szoftverének telepítése után:	Jelentkezzen be a Password Managerbe. A HP ProtectTools Security Managerben kattintson a **Password Manager** elemre, kattintson a **Hitelesítési adatok**, majd az **Intelligens kártya** elemre. Indítsa újra a számítógépet, ha az felszólítja erre.
Egyes alkalmazások weboldalai hibákat generálnak, amelyek megakadályozzák a felhasználót a feladatok végrehajtásában.	Egyes webes alkalmazások leállnak, és hibát jelentenek az egyszeri bejelentkezés letiltási funkcióinak beállítása miatt. Például egy sárga háromszögben látható **!** jelenik meg az Internet Explorer programban, ami azt jelzi, hogy hiba történt.	A Security Manager Egyszeri bejelentkezés nem támogatja az összes szoftveres webes felületet. Tiltsa le az Egyszeri bejelentkezési támogatást az adott weboldalra. Az Egyszeri bejelentkezés teljes dokumentációját lásd a Security Manager szoftver súgójában. Ha az adott alkalmazás adott egyszeri bejelentkezési szolgáltatása nem tiltható le, hívja a HP vevőszolgálatát, és igényelje az adott program támogatását a HP szerviz kapcsolattartóján keresztül.
A **Browse for Virtual Token** (Virtuális token tallózása) lehetőség nem jelenik meg a bejelentkezés során.	A felhasználó nem viheti át a regisztrált virtuális tokenjének helyét a Password Managerben, mert a tallózási lehetőséget a biztonsági kockázatok miatt eltávolították.	A tallózás lehetősége megszűnt, mivel ez bárkinek lehetővé tette a fájlok törlését és átnevezését, ezáltal a Windows irányításának átvételét.
A tartományi rendszergazdák még engedély birtokában sem tudják módosítani a Windows-jelszót.	Ez akkor történik, miután egy tartomány rendszergazdája belép egy tartományba, és regisztrálja a tartományazonosítót a Password Managerrel, egy az adott tartomány vagy helyi PC rendszergazdai fiókja jogainak felhasználásával. Ha egy tartomány rendszergazdája megkísérli megváltoztatni a Windows-jelszót a Password Manageren keresztül, a rendszergazda a következő hibaüzenetet kapja: **Felhasználói fiók korlátozása**.	A Password Managerrel nem lehet az egy adott tartományhoz tartozó felhasználói fiók jelszavát a **Windows-jelszó módosítása** elem segítségével módosítani. A Security Managerrel csak a helyi számítógépen található fiókok jelszava módosítható. Az adott tartományhoz tartozó felhasználó a jelszavát a **Windows biztonság Jelszómódosítás** menüpontján keresztül tudja módosítani, de mivel az adott tartományhoz tartozó felhasználónak nincs valós fiókja a helyi számítógépen, a Password Managerrel csak a belépési jelszó módosítható.
A Password Managernek ismert inkompatibilitási	Ha a felhasználó bejelentkezik a Password Managerbe, létrehoz egy	A HP jelenleg keresi a megoldást erre a problémára.

Rövid leírás	Részletek	Megoldás
problémái vannak a Corel WordPerfect 12 „GINA” jelszóval.	dokumentumot a WordPerfectben, elmenti jelszóvédelemmel, a Password Manager nem fogja felismerni sem kézzel sem automatikusan a GINA jelszót.	
A Password Manager nem ismeri fel a **Kapcsolódás** gombot a képernyőn.	Ha az egyszeri bejelentkezés távoli asztal kapcsolatban (RDP) használt hitelesítő adatainál a **Connect** (Csatlakozás) beállítás szerepel, az egyszeri bejelentkezés újraindításkor a **Save As** (Mentés másként) lehetőségre lép a **Connect** (Csatlakozás) helyett.	A HP jelenleg keresi a megoldást erre a problémára.
A Windows XP 1-es szervizcsomagjánál a felhasználó nem tud belépni a Password Managerbe, miután a rendszer készenléti állapotból hibernált állapotba került.	Miután engedélyezték, hogy a rendszer alvó vagy hibernált állapotba kerüljön, a rendszergazda vagy felhasználó nem tud belépni a Password Managerbe, és a Windows bejelentkezési képernyő marad látható, függetlenül attól, milyenfajta hitelesítés történt (jelszó, ujjlenyomat, Java-kártya).	A Windows frissítése a 2. Szervizcsomaggal a Windows Update használatával. A kérdés okával kapcsolatos további információkért lásd a Microsoft tudásbázis 813301 számú cikkét: http://www.microsoft.com. A bejelentkezéshez a felhasználónak a Password Managert kell kiválasztania. A Password Managerbe való belépés után a felhasználónak be kell jelentkeznie a Windowsba (neki kell kijelölnie a bejelentkezési lehetőséget), hogy a bejelentkezési folyamat végbemenjen. Ha a felhasználó előbb a Windowsba jelentkezik be, saját magának kell gondoskodnia arról, hogy a Password Managerbe is belépjen.
A biztonságos **Restore Identity** (Identitás visszaállítása) folyamat elveszti kapcsolatát a virtuális tokennel.	Ha a felhasználó visszaállítja az azonosítóját, a Password Manager elveszítheti a megfelelő társítást a virtuális token helyével a bejelentkezési képernyőn. Bár a Password Managernek is megvan a saját regisztrált virtuális tokenje, a felhasználónak regisztrálnia kell a tokent, hogy visszaállítsa a társítást.	Jelenleg ez a normális működés. Ha a Security Managert az azonosítók megtartása nélkül távolítja el, a token rendszer (kiszolgálói) része megsemmisül, így a tokent többé nem lehet belépésre használni, még akkor sem, ha a token kliensoldali részét visszaállítják. A HP keresi a probléma hosszú távú megoldási lehetőségeit.

Device Access Manager for HP ProtectTools

A felhasználóknak az Eszközkezelőhöz való hozzáférése meg lett tagadva, de az eszközök még hozzáférhetők.

- **Magyarázat**: az Egyszerű beállítások és/vagy az Eszközosztály beállításait az Eszközkezelőn keresztül használták, hogy felhasználóknak az eszközökhöz való hozzáférését megtagadják. A megtagadott hozzáférések ellenére a felhasználók még mindig hozzáférhetnek az eszközökhöz.
- **Megoldás:**
  - Ellenőrizze, hogy a HP ProtectTools Device Locking szolgáltatás elindult-e.
  - Rendszergazdaként kattintson a **Vezérlőpult**, majd a **Felügyeleti eszközök** lehetőségre. A Felügyeleti eszközök ablakban kattintson a **Szolgáltatások** pontra, majd keressen rá a **HP ProtectTools Device Locking/Auditing** szolgáltatásra. Győződjön meg róla, hogy a szolgáltatás elindult, és hogy az indítás típusa **Automatikus**-e.

Egy felhasználónak nem várt hozzáférése van egy eszközhöz, illetve váratlan módon meg van tagadva a hozzáférése egy eszközhöz.

- **Magyarázat**: az Eszközkezelőt arra használták, hogy engedélyeket adjanak vagy megtagadjanak bizonyos felhasználóknak bizonyos eszközökhöz. Amikor a felhasználó használja a rendszert, hozzáfér olyan eszközökhöz, amelyekhez az Eszközkezelő szerint nem kellene, és nem fér hozzá olyan eszközökhöz, amelyekhez az Eszközkezelő szerint hozzá kellene férnie.
- **Megoldás:**
  - Használja az Eszközosztály beállításait az Eszközkezelőben, hogy kiderítse a felhasználó eszközbeállításait.
  - Kattintson a **Security Manager**, az **Eszközkezelő**, majd az **Eszközosztály beállításai** lehetőségre. Nyissa ki az Eszközosztály hierarchiájában a szinteket, hogy kiderítse a felhasználóra vonatkozó beállításokat. Nézze meg, hogy nincs-e „Megtagadás” beállítás a felhasználón vagy bármely Windows csoporton, amelynek a felhasználó a tagja (pl. Felhasználók, Rendszergazdák).

Engedélyezés, megtagadás: melyik élvez elsőbbséget?

- **Magyarázat**: az Eszközosztály beállításain belül a következő beállítások vannak:
  - Az Engedélyezés egy Windows-csoporthoz (pl. BUILTIN\Rendszergazdak), az Engedélyezés megtagadása pedig egy másik Windows-csoporthoz (pl. BUILTIN\Felhasznalok) tartozik az eszközosztály-hierarchia azonos szintjén (pl. DVD/CD-ROM-meghajtók).
  - Ha egy felhasználó két csoportnak is tagja (pl. Rendszergazda), melyik élvez elsőbbséget?
- **Megoldás:**
  - A felhasználó hozzáférése meg lesz tagadva. A megtagadás elsőbbséget élvez az engedélyezés felett.
  - A hozzáférés meg lesz tagadva. Ennek oka a Windows engedélyezési algoritmusa. Egy csoport hozzáférése meg van tagadva, egy másiké engedélyezve van, de a felhasználó mindkét csoport tagja. A felhasználó hozzáférése meg lesz tagadva, mert a megtagadás elsőbbséget élvez az engedélyezési jogok felett.

- Kisegítő megoldás lehet, ha megtagadja a Felhasználók csoportot a DVD/CD-ROM-meghajtók szintjén, és engedélyezi a Rendszergazdák csoportot a DVD/CD-ROM-meghajtók szintje alatt.
- Más megoldás lehet, hogy Windows-csoportokat hoz létre. Egyet, amelyhez enged hozzáférést a DVD/CD-hez, és egy másikat, amelynek a DVD/CD-hez való hozzáférését megtagadja. A felhasználókat ezentúl a megfelelő csoporthoz kell hozzáadni.

Az Egyszerű beállítások nézetet használták, hogy egy eszköz hozzáférési házirendjét meghatározzák, de a rendszergazdai felhasználók nem férnek hozzá az eszközökhöz.

- **Magyarázat**: az Egyszerű beállítások megtagadja a hozzáférést a Felhasználók és Vendégek számára, és engedélyezi az Eszköz rendszergazdái számára.
- **Megoldás:** Adja hozzá a rendszergazdai felhasználót az Eszköz rendszergazdái csoporthoz.

Egyéb

A szóban forgó szoftver – Rövid leírás	Részletek	Megoldás
Security Manager – a következő figyelmeztetés jelent meg: **The security application can not be installed until the HP Protect Tools Security Manager is installed** (A biztonsági alkalmazást nem lehet telepíteni, amíg a Hp ProtectTools Security Manager program nincs telepítve).	Minden biztonsági alkalmazás, mint például a Java Card Security és a biometrikus rendszerek kiegészítőként használhatók a Security Manager felületén. A Security Managert előbb kell telepíteni, minthogy a HP által jóváhagyott biztonsági kiegészítő betöltődne.	A HP által jóváhagyott biztonsági beépülő modulokat a Security Manager program telepítése után lehet betölteni.
HP ProtectTools Security Manager – Időnként hibaüzenet jelenik meg a Security Manager kezelőfelületének bezárása után.	Időnként (12 esetből kb. egyszer) hibaüzenet jelenik meg, ha a Security Manager program ablakát azelőtt zárják be a jobb felső sarokban látható bezárás gombbal, hogy a beépülő modulok betöltődtek volna.	Ez a probléma a Security Manager bezárásakor és újraindításakor a beépülő modulok betöltésének időzítésével van összefüggésben. Mivel a PTHOST.exe az a héj, amely más alkalmazásokat (beépülő modulokat) futtat, működése függ attól, hogy a beépülő modulok (szolgáltatások) mennyi idő alatt képesek betöltődni. A problémát a héj bezárása okozza még azelőtt, hogy a beépülő modul betöltődött volna. Hagyjon időt arra, hogy a Security Manager megjelenítse a szolgáltatások betöltődését jelző üzenetet (amely a Security Manager ablakának felső részén látható), és minden beépülő modult megjelenjen a bal oszlopban. A hibát úgy kerülheti el, hogy elegendő időt hagy a beépülő modulok betöltésére.
HP ProtectTools – A korlátlan hozzáférés vagy szabályozatlan rendszergazdai jogosultságok biztonsági kockázatot jelentenek.	Ha az ügyfélszámítógép korlátozás nélkül elérhető, a következő kockázatoknak van kitéve: • A PSD meghajtó törlése • A felhasználói beállítások rosszindulatú módosítása • A biztonsági házirend és funkciók letiltása	A rendszergazdák a legmegfelelőbb gyakorlatnak megfelelően dönthetnek a végfelhasználói jogosultságok, illetve a hozzáférések korlátozásáról. Az illetéktelen felhasználók nem kaphatnak rendszergazdai jogosultságot.

Szószedet

aktiválás Az a feladat, amelynek be kell fejeződnie, mielőtt a meghajtótitkosítási szolgáltatás elérhetővé válik. A meghajtótitkosítást a HP ProtectTools Telepítő varázsló használatával aktiválták. Csak rendszergazda aktiválhatja a meghajtótitkosítást. Az aktiválási folyamat a következőkből áll: a szoftver aktiválása, a meghajtó titkosítása, a felhasználói fiók létrehozása és egy kezdeti biztonsági mentés létrehozása a titkosító kódról egy eltávolítható tárhelyen.

Aláírás és titkosítás gomb Szoftveres gomb, amely megjelenik a Microsoft Outlook alkalmazásainak eszköztárán. Ha a gombra kattint, aláírhatja, titkosíthatja vagy visszafejtheti a Microsoft Office dokumentumokat.

aláírási sor A digitális aláírás vizuális megjelenítésének helyfoglalója. Ha egy dokumentumot aláírnak, megjelenik az aláíró neve és az ellenőrzés módja. Az aláírás dátuma és az aláíró titulusa is megjelenik.

ATM Automatic Technology Manager, amelynek segítségével a hálózati rendszergazdák távolról, a BIOS szintjén is tudnak rendszereket üzemeltetni.

áttekintőlap Egy központi hely, ahol elérheti és kezelheti a funkciókat és beállításokat a HP ProtectTools Security Manager szoftverben.

áttelepítés Feladat, amely lehetővé teszi a Privacy Manager Certificates és Trusted Contacts kezelését, helyreállítását és áthelyezését.

automatikus foszlatás Beütemezett foszlatás, amelyet a felhasználó a Fájlürítő alkalmazásban állít be.

bejelentkezés A Security Manager egy objektuma, amely tartalmaz egy felhasználói nevet és jelszót (és esetleg más információt), amelyekkel a felhasználó webhelyekre vagy más programokba tud belépni.

bélyegző a megbízható kapcsolatokhoz Feladat, amely hozzáad egy digitális aláírást, titkosítja az e-mailt és elküldi azt, miután Ön a kiválasztott biztonsági bejelentkezési üzemmód használatával hitelesítette.

billentyűsorozat Megadott gombok kombinációja, amelyeknek lenyomása kivált egy automatikus foszlatást—például ctrl+alt+s.

biometrikus Olyan hitelesítő adatok kategóriája, amelyek fizikai tulajdonságot, például ujjlenyomatot használnak egy felhasználó azonosítására.

biztonsági bejelentkezési eljárás A számítógépbe való bejelentkezéshez használt eljárás.

biztonsági mentés A biztonsági mentéssel a program fontos információiról másolatot menthet egy a programon kívüli helyre. Ez később felhasználható az információk visszaállításához ugyanezen vagy egy másik számítógépen.

Biztonságos küldés gomb Szoftveres gomb, amely megjelenik a Microsoft Outlook e-mail üzeneteinek eszköztárán. A gombra kattintva aláírhatja és/vagy titkosíthatja Microsoft Outlook e-mailes üzeneteit.

csevegéselőzmények Titkosított fájl, amely tartalmazza egy csevegési munkamenetben lezajlott beszélgetés mindkét oldalát.

csoport Olyan felhasználók csoportja, akiknek azonos szintű hozzáférése van egy eszközhöz vagy eszközosztályhoz.

dekódolás A kriptográfiában használt eljárás a titkosított adatok sima szöveggé alakításához.

digitális aláírás A fájllal együtt elküldött adatok, amelyek igazolják az anyag küldőjét és azt, hogy a fájlt nem módosították az aláírást követően.

digitális tanúsítvány Elektronikus hitelesítő adatok, amelyek megerősítik egy személy vagy társaság személyazonosságát azáltal, hogy a digitális tanúsítvány tulajdonosát összekapcsolják egy olyan elektronikus kulcspárral, amely digitális információk aláírására szolgálnak.

Drive Encryption bejelentkezési képernyő Egy bejelentkezési képernyő, ami a Windows elindulása előtt jelenik meg. A felhasználóknak meg kell adniuk Windows felhasználónevüket és jelszavukat vagy a Java-kártya PIN-kódját. A legtöbb esetben a helyes információ beírása a Drive Encryption bejelentkezési képernyőjén anélkül is lehetővé teszi a közvetlen hozzáférést a Windowshoz, hogy ismét be kellene lépni a Windows bejelentkezési képernyőjén.

DriveLock Biztonsági szolgáltatás, amely összekapcsolja a merevlemez-meghajtót egy felhasználóval, és megköveteli, hogy a felhasználó pontosan beírja a DriveLock jelszót, amikor a számítógép elindul.

Egyszeri bejelentkezés Szolgáltatás, amely hitelesítési információkat tárol, és lehetővé teszi a Security Manager használatát az internet és olyan Windows-alkalmazások eléréséhez, amelyek jelszavas hitelesítést igényelnek.

egyszerű törlés Erőforrásra mutató Windows hivatkozás törlése. Az erőforrás tartalma a merevlemez-meghajtón marad mindaddig, amíg az összezavart adatokat felül nem írja a szabad hely kifehérítése.

erőforrás Adatelem, amely személyes információkat vagy fájlokat, előzményekkel és internettel kapcsolatos adatokat stb. tartalmaz, és amely a merevlemezen található.

eszköz-hozzáférési házirend Eszközök listája, amelyekhez egy felhasználó hozzáférése engedélyezve van vagy meg van tagadva.

eszközosztály Egy adott típus összes eszköze (például meghajtók).

felfedés Feladat, amely lehetővé teszi, hogy a felhasználó visszafejtsen egy vagy több csevegési munkamenet előzményt, egyszerű szövegként jelenítve meg a Kapcsolat-képernyőnevet/neveket, és hozzáférhetővé téve a munkamenetet megtekintés céljából.

felhasználó Olyan személy, akinek van jogosultsága a Drive Encryption alkalmazáshoz. A rendszergazdai jogosultságokkal nem rendelkező felhasználóknak korlátozott jogosultságuk van a Drive Encryption szoftverhez. Ők (rendszergazdai engedéllyel) csak feliratkozhatnak és bejelentkezhetnek.

foszlatás Egy algoritmus végrehajtása, amely összezavarja az erőforrásban lévő adatokat.

foszlatási ciklus Az a szám, ahányszor a foszlatási algoritmust az egyes erőforrásokon végrehajtják. Minél magasabb számot választ ki a foszlatási ciklushoz, annál biztonságosabb lesz a számítógép.

foszlatási profil A megadott törlési módszer és az erőforrások listája.

hálózati fiók Windows felhasználói vagy rendszergazdai fiók, egy munkacsoport helyi számítógépén vagy egy tartományban.

háttérszolgáltatás A HP ProtectTools Device Locking/Auditing háttérszolgáltatás, amelynek futnia kell az eszköz-hozzáférési házirendek alkalmazásához. A szolgáltatás állapota a Vezérlőpult Felügyeleti eszközök alkalmazásának Szolgáltatások részében tekinthető meg. Ha a szolgáltatás nem fut, a HP ProtectTools Security Manager megpróbálja elindítani, amikor az eszköz-hozzáférési házirendeket alkalmazzák.

hitelesítés Annak ellenőrzése, hogy egy adott felhasználó jogosult-e az olyan feladatok végrehajtására, mint egy számítógép elérése, adott program beállításainak módosítása vagy titkos adatok megtekintése.

hitelesítési adatok Módszer, amellyel egy felhasználó jogosultságot szerez egy bizonyos feladatra a hitelesítési eljárás keretében.

hitelesítésszolgáltató Szolgáltató, amely kiadja a nyilvános kulcson alapuló infrastruktúra használatához szükséges tanúsítványokat.

hitelesített felhasználó Olyan felhasználó, akinek engedélyt adtak a Felhasználói hozzáférések beállításaiban az Egyszerű beállítások vagy Eszközosztályok beállításai nézeteinek megtekintésére vagy módosítására.

HP SpareKey A merevlemez titkosító kódjának biztonsági másolata.

identitás A HP ProtectTools Security Manager szoftverben olyan hitelesítési adatok és beállítások csoportja, amelyek egy bizonyos felhasználó fiókjaként vagy profiljaként kerülnek kezelésre.

intelligens kártya Kisméretű hardver, méretében és alakjában a hitelkártyához hasonló, amely a tulajdonos azonosítására szolgáló adatokat tartalmaz. A tulajdonos számítógépen történő azonosításához használatos.

Java-kártya A számítógépbe helyezett kivehető kártya. Azonosítási adatokat tartalmaz a bejelentkezéshez. Ha Java-kártyával szeretne bejelentkezni a Drive Encryption bejelentkezési képernyőn, be kell helyeznie a Java-kártyát és be kell írnia felhasználói nevét és a Java-kártya PIN-kódját.

javasolt aláíró Aláíró, akit a Microsoft Word vagy Microsoft Excel dokumentum tulajdonosa arra jelölt ki, hogy aláírási sort adjon hozzá a dokumentumhoz.

kép Egy felvett felhasználóról készült, hitelesítéshez használt fénykép.

kézi foszlatás Egy erőforrás vagy kiválasztott erőforrások azonnali foszlatása, ami megkerüli az automatikus foszlatás ütemtervét.

kommunikáció megbízható azonnali üzenetküldő programokon keresztül Kommunikációs munkamenet, amelynek során megbízható üzeneteket küldenek egy megbízható feladótól egy megbízható kapcsolathoz.

konzol Egy központi hely, ahol elférheti és kezelheti a funkciókat és beállításokat a HP ProtectTools Administrative Console alkalmazásban.

kriptográfia Az adatok titkosításának és visszafejtésének gyakorlata úgy, hogy csak bizonyos személyek dekódolhassák.

kriptográfiai szolgáltató (CSP) Olyan kriptográfiai algoritmusokat biztosító szervezet vagy könyvtár, amely jól meghatározott felületen keresztül használhatók bizonyos kriptográfiai műveletek végrehajtására.

Live Messenger előzmények megtekintése A Privacy Manager Chat egyik eleme, amely lehetővé teszi titkosított csevegési munkamenet-előzmények keresését és megjelenítését.

megbízható feladó Megbízható kapcsolat, aki aláírt és/vagy titkosított e-maileket és Microsoft Office dokumentumokat küld.

Megbízható kapcsolat Olyan személy, aki elfogadott egy megbízható kapcsolat-meghívást.

Megbízható kapcsolat, meghívó Adott személy számára elküldött e-mail, amely felkérést tartalmaz a megbízható kapcsolat elfogadására.

Megbízható kapcsolat címzettje Olyan személy, aki felkérést kap megbízható kapcsolati felkérés elfogadására.

Megbízható kapcsolatok listája A megbízható kapcsolatok felsorolása.

megbízható üzenet Kommunikációs munkamenet, amelynek során megbízható üzeneteket küldenek egy megbízható feladótól egy megbízható kapcsolathoz.

Meghajtótitkosítás Megvédi adatait a merevlemez(ek) titkosításával oly módon, hogy az információk olvashatatlanok lesznek az engedély nélküli felhasználók számára.

Névjegykártya Windows Oldalsáv-alkalmazás, amely segít az asztal vizuálisan azonosításában egy felhasználói név és kép felhasználásával. Kattintson a névjegykártyára a HP ProtectTools Administrative Console megnyitásához.

PIN-kód Személyes azonosító szám.

PKI Nyilvános kulcsú infrastruktúra-szabvány, amely meghatározza a tanúsítványok és kriptográfiai kulcsok létrehozásához, használatához és adminisztrálásához használható felületet.

Privacy Manager-tanúsítvány Digitális tanúsítvány, amely minden alkalommal megköveteli a hitelesítést, amikor titkosítási műveletekhez használja, például e-mailek és Microsoft Office dokumentumok aláírása és titkosítása.

PSD Biztonságos személyi meghajtó, amely védett tárhelyként szolgál a bizalmas adatok számára.

rendszergazda *Lásd* Windows rendszergazda.

rendszerindításkori hitelesítés Biztonsági elem, amely a számítógép bekapcsolásakor a hitelesítés valamilyen formáját igényli, például a Java-kártyát, a biztonsági lapkát vagy egy jelszót.

SATA-eszköz mód Adatátviteli üzemmód a számítógép és tömegtár-eszközök, például merevlemez-meghajtók és optikai meghajtók között.

szabad hely kifehérítése A kiválasztott erőforrások véletlenszerű adatokkal történő titkos felülírása a törölt erőforrások tartalmának eltorzítására.

tartomány Számítógépek csoportja, amelyek egy hálózat részei és közös könyvtár-adatbázison osztoznak. A tartományok egyedi nevet viselnek, és mindegyikre közös szabályok és eljárások vonatkoznak.

titkosítás Eljárás, például egy algoritmus használata, amelyet a kriptográfiában használnak sima szöveg titkosított szöveggé alakításához annak érdekében, hogy az illetéktelen címzettek ne ismerhessék meg az adattartalmat. Sokféle adattitkosítás létezik, és ezek alkotják a hálózati biztonság alapját. Gyakori típus például a DES (Data Encryption Standard = adattitkosítási szabvány) és a nyilvános kulcsú titkosítás.

titkosított fájlrendszer (EFS) Olyan fájlrendszer, amely minden fájlt és almappát titkosít a kiválasztott mappában.

token Lásd biztonsági belépési eljárás

TXT Trusted Execution Technology (megbízható végrehajtási technológia).

ujjlenyomat Az ujjlenyomat digitális képe. Az ujjlenyomat valódi képét a Security Manager nem tárolja.

újraindítás A számítógép újraindításának folyamata.

USB-token Biztonsági eszköz, amely azonosító információkat tárol egy felhasználóról. A Java-kártyához és a biometriai leolvasóhoz hasonlóan a számítógép tulajdonosának hitelesítésére szolgál.

vész-helyreállítási archívum Védett tárolóterület, amely lehetővé teszi az alapfelhasználói kulcsok újrakódolását egyik platformtulajdonosi kulcsból egy másikba.

virtuális token Biztonsági szolgáltatás, amely a Java-kártyához és a kártyaolvasóhoz nagyon hasonlóan működik. A token vagy a számítógép merevlemezén, vagy pedig a Windows rendszerleíró adatbázisában van

mentve. Ha virtuális token használatával jelentkezik be, a hitelesítés elvégzéséhez a számítógép felszólítja Önt felhasználói PIN-kód megadására.

visszaállítás Az az eljárás, amellyel előzőleg biztonsági okokból elmentett programinformációkat visszamásolunk a programba.

visszavonási jelszó Ez a jelszót akkor jön létre, amikor a felhasználó digitális tanúsítványt igényel. A jelszóra akkor van szükség, ha a felhasználó szeretné visszavonni digitális tanúsítványát. Ez lehetővé teszi, hogy csak a felhasználó vonhassa vissza a tanúsítványt.

Windows felhasználói fiók Olyan személy profilja, aki bejelentkezhet a hálózatba vagy egy egyedi számítógépre.

Windows Logon Security A Windows Logon Security alkalmazás biztosítja a Windows fiók(ok) védelmét, mivel a felhasználóktól adott hitelesítési adatokat kíván meg a belépéshez.

Windows rendszergazda Korlátlan jogosultsággal rendelkező felhasználó engedélyek módosítására és más felhasználók menedzselésére.

Tárgymutató

F

H

I

J

K

W