HP Client Security

Első lépések

Az itt szereplő információ előzetes értesítés nélkül változhat. A HP termékeire és szolgáltatásaira vonatkozó kizárólagos jótállás az adott termékhez, illetve szolgáltatáshoz mellékelt, korlátozott jótállásról szóló nyilatkozatban vállalt jótállás. A dokumentumban ismertetettek nem jelentenek semmiféle további jótállást. A HP nem vállal felelősséget az itt található esetleges technikai vagy szerkesztési hibákért és mulasztásokért.

Első kiadás: 2013. augusztus

A dokumentum cikkszáma: 735339-211

Tartalomjegyzék

1 Bevezetés a HP Client Security Manager-be

A HP Client Security lehetővé teszi adatai, eszköze és személyazonossága védelmét, és ezáltal növeli számítógépe biztonságát.

A számítógépe részére elérhető szoftvermodulok a modelltől függően változhatnak.

A HP Client Security szoftvermodulok lehetnek előretelepítettek, előre betöltöttek vagy letöltésre elérhetők a HP weboldalról. További tudnivalók: http://www.hp.com.

MEGJEGYZÉS: Jelen útmutatóban az utasításokat azon feltételezéssel írtuk, hogy már telepítette az adott HP Client Security szoftvermodulokat.

HP Client Security tulajdonságai

Az alábbi táblázat a HP Client Security modulok fontosabb tulajdonságait részletezi.

Modul	Fontosabb tulajdonságok
HP Client Security Manager	A rendszergazdák az alábbi funkciókat végezheti el: • Védje számítógépét mielőtt elindul a Windows®. • Védje a Windows fiókját erős hitelesítéssel. • Kezelje a bejelentkezési adatait és jelszavait a weboldalakhoz és alkalmazásokhoz. • Könnyen módosítsa a Windows operációs rendszer jelszavát. • Használjon ujjlenyomatokat az extra biztonsághoz és a kényelemhez • Helyezzen üzembe intelligens kártyákat, érintkezés nélküli kártyákat vagy közelségérzékelő kártyákat a hitelesítéshez • Használja a Bluetooth-telefonját azonosítási módszerként • Állítson be PIN-kódot úgy, hogy kiterjessze a hitelesítési választékát • Konfigurálja a bejelentkezési szabályokat és munkamenet házirendet • Készítsen biztonsági mentést, és állítsa vissza a programadatokat • Adjon hozzá több alkalmazást, például: HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP eszközhozzáférés-kezelő és HP CompuTrace Az általános felhasználók az alábbi funkciókat végezhetik el: • Megnézhetik az Encryption Status és a Device Access Manager beállításait. • Aktiválhatják a Computrace-t. • Konfigurálhatják a Beállítások és Biztonsági mentés és visszaállítás opciókat.
Password Manager	Az általános felhasználók az alábbi funkciókat végezhetik el: • Rendszerezhetik és beállíthatják a felhasználóneveket és jelszavakat. • Létrehozhatnak erősebb jelszavakat a nagyobb fiókbiztonság érdekében az e-mailek és webes fiókok esetében. A Password Manager automatikusan kitölti és beküldi az adatokat. • Egyszerűsítheti a bejelentkezési folyamatot a Single Sign On funkcióval, amely automatikusan emlékszik a felhasználó hitelesítő adataira, és azokat alkalmazza. • Megjelölhet egy fiókot kompromittáltként úgy, hogy figyelmezteti Önt más fiók(ok)ra hasonló hitelesítő adatokkal. • Beimportálhat bejelentkezési adatokat támogatott böngészőkből.
HP Drive Encryption (csak bizonyos modelleknél)	• Teljes, egész térfogatos merev lemez titkosítást biztosít. • Erőlteti a bootlolás előtti hitelesítést, hogy kikódolja és hozzáférjen az adatokhoz. • Lehetőséget nyújt az öntitkosító meghajtók aktiválására (csak bizonyos modellek).

Modul	Fontosabb tulajdonságok
HP eszközhozzáférés-kezelő	• Lehetővé teszi, hogy az IT vezetők a felhasználói profilok alapján szabályozzák az eszközökhöz való hozzáférést. • Megakadályozza, hogy engedéllyel nem rendelkező felhasználók adatokat távolítsanak el külső tárolóeszköz segítségével, illetve, hogy vírusokat vigyen a rendszerbe külső eszközről. • Lehetővé teszi, hogy a rendszergazdák letiltsák bizonyos személyek vagy felhasználói csoportok hozzáférését a kommunikációs eszközökhöz.
HP Trust Circles	• Biztosítja a fájlok és dokumentumok biztonságát. • Titkosítja a felhasználóra jellemző mappákban található fájlokat, és megbízható körökön belül védi azokat. • Lehetővé teszi, hogy a fájlokat kizárólag a megbízható körön belüli tagok között használhassák és oszthassák meg.
Theft Recovery (Computrace, külön vásárolható)	• A követő és jelölő feliratkozásokat külön meg kell vásárolni az aktiváláshoz. • Biztonságos forráskövetést biztosít. • Figyeli a felhasználó tevékenységét, illetve a hardver és szoftver változásait. • Még akkor is aktív marad, ha a merev lemezt újraformázzák vagy kicserélik.

A HP Client Security termék leírása és példák a szokásos felhasználásra

A legtöbb HP Client Security termék egyaránt rendelkezik felhasználóhitelesítéssel (általában jelszóval) és rendszergazdai biztonsági mentéssel, hogy a hozzáférés visszanyerhető lehessen, ha a jelszavak elvesznek, nem elérhetőek vagy azokat elfelejtett, illetve bármikor, amikor a vállalati biztonságnak szüksége van a hozzáférésre.

MEGJEGYZÉS: A HP Client Security termékek közül néhányat az adathozzáférés korlátozására terveztek. Az adatokat titkosítani kell, amikor olyan fontosak, hogy a felhasználó inkább elveszítené az információt, semmint, hogy azokat kompromittálják. Javasolt az összes adatról biztonsági másolatot készíteni egy biztonságos helyen.

Password Manager

A Password Manager tárolja a felhasználóneveket és jelszavakat, és az alábbiakra használható:

- Elmenti a bejelentkezési neveket és jelszavakat az Internet eléréséhez vagy az e-mailekhez.
- Automatikusan bejelenti a felhasználót egy weboldalra vagy e-mail fiókba.
- Kezeli és rendszerezi a hitelesítéseket.
- Webes vagy hálózati forrást választ ki, és közvetlenül eléri a hivatkozást.
- Megtekinti a neveket és jelszavakat, amikor szükséges.

- Megjelölhet egy fiókot kompromittáltként úgy, hogy figyelmezteti Önt más fiók(ok)ra hasonló hitelesítő adatokkal.
- Beimportálhat bejelentkezési adatokat támogatott böngészőkből.

1. példa: Egy nagy gyártó kereskedelmi ügynöke a vállalati tranzakcióinak legnagyobb részét az Interneten bonyolítja. Gyakran látogat több népszerű weboldalt is, melyhez bejelentkezési adatokra van szükség. Nagyon jól tisztában van a biztonsággal, hogy nem használhatja ugyanazt a jelszót minden fiókhoz. A kereskedelmi ügynök úgy határozott, hogy a Password Manager alkalmazást használja a webes hivatkozások különböző felhasználónevekkel és jelszavakkal való illesztéséhez. Amikor egy weboldalra megy, hogy bejelentkezzen, a Password Manager automatikusan megjeleníti a hitelesítő adatokat. Ha meg szeretné nézni a felhasználóneveket és jelszavakat, akkor a Password Manager konfigurálható ezek megmutatására.

A Password Manager használható hitelesítések kezelésére és rendszerezésére is. Ez az eszköz lehetővé teszi, hogy a felhasználó kiválasszon egy webes vagy hálózati forrást, és közvetlenül hozzáférjen a hivatkozáshoz. A felhasználó meg is tekintheti a felhasználóneveket és jelszavakat, amikor szükséges.

2. példa: Egy keményen dolgozó alkalmazottat előléptettek, és most a teljes könyvelési osztályt vezeti. A csapatnak sok kliens webes fiókjába kell bejelentkeznie, amely felhasználók mindegyikének különböző a bejelentkezési adata. Ezt a bejelentkezési információt meg kell osztani más dolgozókkal, azaz a titoktartás probléma. Az alkalmazott úgy dönt, hogy az összes webes hivatkozást, vállalati felhasználónevet és jelszót rendszerezi a Password Manager segítségével. Amint készen van, az alkalmazott beveti a Password Manager-t az dokgozóknak, hogy a webes fiókokon dolgozhassanak és soha ne tudják meg a bejelentkezés hitelesítő adatait, melyeket használnak.

HP Drive Encryption (csak bizonyos modelleknél)

A HP Drive Encryption használatos az adatokhoz való hozzáférés korlátozására a teljes számítógép-merevlemezen vagy másodlagos lemezen. A Drive Encryption kezelni tudja az öntitkosító meghajtókat is.

1. példa: Egy orvos szeretne meggyőződni arról, hogy csak ő tud hozzáférni az adatokhoz a számítógépe merevlemezén. Az orvos aktiválja a Drive Encryption alkalmazást, melyhez a Windows-ba való bejelentkezés előtt, rendszerindítás előtti hitelesítés szükséges. Amint beállította, a merevlemez nem érhető el jelszó nélkül az operációs rendszer elindítása előtt. Az orvos tovább növelheti a meghajtó biztonságát, ha az öntitkosító meghajtó opcióval kiválasztja az adatok titkosítását.

2. példa: Egy kórházi rendszergazda szeretné biztosítani, hogy csak orvosok és engedéllyel rendelkező személyek férhessenek hozzá a helyi számítógép adataihoz, anélkül, hogy a személyes jelszavaikat meg kellene osztaniuk. Az IT osztály hozzáadja a rendszergazdát, az orvosokat és az összes engedéllyel rendelkező személyt Drive Encryption felhasználókként. Most csak az engedéllyel rendelkező személyek indíthatják el a számítógépet vagy domént a személyes felhasználónevüket és jelszavukat használva.

HP Device Access Manager (csak bizonyos modelleknél)

A HP Device Access Manager lehetővé teszi, hogy a rendszergazdák korlátozzák és kezeljék a harver hozzáférését. A Device Access Manager nem engedélyezett hozzáférések blokkolására használható olyan USB flash meghajtókhoz, ahol az adatok másolhatók. Korlátozhatja a hozzáférést a CD/DVD meghajtókhoz, szabályozhatja az USB-s eszközöket, hálózati csatlakozásokat stb. Egy példa helyzet, amikor külsős vállalkozónak kell hozzáfernie a vállalati számítógépekhez, de nem másolhatja az adatokat USB meghajtóra.

1. példa: Egy gyógyszerellátó cég vezetője gyakran dolgozik személyes orvosi feljegyzésekkel a vállalat információi mellett. Az alkalmazottaknak hozzá kell férniük ezekhez az adatokhoz, de

különösen fontos, hogy az adatok nem tünjenek el a számítógépről USB meghajtó vagy más külső tárolóeszköz segítségével. A hálózat biztonságos, de a számítógépekben vannak CD-írók és USB-portok, melyek lehetővé tehetik az adatok másolását vagy ellopását. A vezető a Device Access Manager segítségével tiltja le az USB-portokat és a CD-írókat, hogy ne legyenek használhatók. Bár az USB-portok blokkoltak, az egér és a billentyűzet továbbra is használható.

2. példa: Egy biztosítótársaság nem szeretné, hogy alkalmazottai személyes szoftvereket vagy adatokat telepítsenek vagy töltsenek be, otthonukból. Néhány alkalmazottnak hozzá kell férnie az USB-porthoz az összes számítógépen. Az IT vezető a Device Access Manager segítségével engedélyezi néhány alkalmazottnak a hozzáférést, míg blokkolja mások külső hozzáférését.

Computrace (külön vásárolható)

A Computrace (külön vásárolható) olyan szolgáltatás, melyen nyomon tudja követni egy ellopott számítógép helyét, amint a felhasználó használja az Internetet.. A Computrace segíthet távolról irányítani a számítógépet, és meghatározni a helyét, illetve figyelni a számítógép használatát és alkalmazásait.

1. példa: Egy iskolai alapelv arra utasította az IT osztályt, hogy nyomon kövesse az iskolájukban az összes számítógépet. A számítógépek leltározása után az IT rendszergazda regisztrálta az összes számítógépet a Computrace segítségével, így nyomon tudja követni, ha valamikor ellopnák. Nemrég vette észre az iskola, hogy több számítógép hiányzik, így az IT rendszergazda riasztotta a hatóságokat és a Computrace hivatalnokait. A számítógépek helyzetét meghatározták, és azokat a hatóságok visszjutatták az iskolába.

2. példa: Egy ingatlanközvetítő cégnek a világ bármely részén kezelnie és frissítenie kell a számítógépeket. A Computrace segítségével figyelik és frissítik a számítógépeket anélkül, hogy IT személyt kellene küldeniük az adott számítógéphez.

A fontosabb biztonsági célok elérése

A HP Client Security modulok együótt tudnak dolgozni, hogy megoldással szolgáljanak sokféle biztonsági problémára, beleértve az alábbi fontosabb biztonsági célokat:

- Védelem célzott lopás ellen
- Hozzáférés korlátozása érzékeny adatokhoz
- Nem engedélyezett hozzáférés megakadályozása belső vagy külső helyekről
- Erős jelszó-irányelvek létrehozása

Védelem célzott lopás ellen

Célzott lopásra példa lehet egy számítógép ellopása, mely bizalmas adatokat tartalmaz és fogyasztói információkat a repülőtér biztonsági ellenőrző pontjánál. Az alábbi tulajdonságok segítenek védekezni a célzott lopás ellen:

- A rendszerindítás előtti hitelesítő funkció, ha engedélyezett, segít megakadályozni a hozzáférést az operációs rendszerhez.
  - HP Client Security—Lásd: HP Client Security, 13. oldal.
  - HP Drive Encryption—Lásd: HP Drive Encryption (csak bizonyos modelleknél), 31. oldal.
- A titkosítás segít abban, hogy az adatokhoz ne lehessen hozzáférni még akkor sem, ha a merevlemezt kiveszik és nem biztonságos rendszerbe telepítik.
- A Computrace nyomon tudja követni a számítógép helyét egy lopás után.
  - Computrace—Lásd: Lopás helyreállítása (csak bizonyos modelleknél), 55. oldal.

Hozzáférés korlátozása érzékeny adatokhoz

Tételezzük fel, hogy egy szerződéses auditor a helyszínen dolgozik, és számítógépes hozzáférést kapott az érzékeny pénzügyi adatok áttekintése céljából. Nem szeretné, hogy az auditor ki tudja nyomtatni a fájlokat, vagy el tudja azokat menteni írható eszközre, például CD-re. Az alábbi tulajdonság segít korlátozni az adatokhoz való hozzáférést:

- A HP Device Access Manager lehetővé teszi, hogy az IT vezetők korlátozzák a kommunikációs eszközökhöz a hozzáférést, hogy az érzékeny adatokat ne lehessen másolni a merevlemezről.. Lásd: Rendszernézet, 45. oldal.

Nem engedélyezett hozzáférés megakadályozása belső vagy külső helyekről

Az engedély nélküli hozzáférés nem biztonságos céges számítógéphez nagyon valós kockázatot jelent a vállalati hálózati forrásokra, azaz a pénzügyi szolgáltatásokról, végrehajtó vagy kutatási és fejlesztő csapatoktól származó információkhoz és magán adatokhoz, például beteg kórlapjához vagy személyes pénzügyi jegyzékekhez. Az alábbi tulajdonságok segítenek megakadályozni az engedély nélküli hozzáférést:

- A rendszerindítás előtti hitelesítő funkció, ha engedélyezett, segít megakadályozni a hozzáférést az operációs rendszerhez. (lásd: HP Drive Encryption (csak bizonyos modelleknél), 31. oldal.
- A HP Client Security segít biztosítani, hogy az engedéllyel nem rendelkező felhasználók ne kapjanak jelszavakat vagy hozzáférést a jelszóval védett alkalmazásokhoz. Lásd: HP Client Security, 13. oldal.
- A HP Device Access Manager lehetővé teszi, hogy az IT vezetők korlátozzák az írható eszközökhöz a hozzáférést, hogy az érzékeny adatokat ne lehessen másolni a merevlemezről.. Lásd: HP Device Access Manager (csak bizonyos modelleknél), 44. oldal.

Erős jelszó-irányelvek létrehozása

Ha egy vállalati irányelv hatályba kerül, és ez az erős jelszavak irányelvének használatát igényli tucatnyi webalapú alkalmazáshoz és adatbázishoz, akkor a Password Manager biztosítja a jelszavak biztonságos tárolását és a Single Sign On kényelmét. Lásd: Password Manager, 19. oldal.

További biztonsági elemek

Biztonsági szabályok kijelölése

A számítógép-biztonság kezelésében (különösen nagy szervezetek esetén) egy fontos gyakorlat a felelősségek és jogok felosztása különböző típusú rendszergazdák és felhasználók között.

MEGJEGYZÉS: Kis szerevezetknél vagy egyéni használat esetén ezek a szerepek mind egy személynél tarthatók.

A HP Client Security esetében a biztonsági feladatok sé privilégiumok az alábbi szerepekhez oszthatók fel:

- Biztonsági hivatalnok—Meghatározza a vállalat vagy hálózat biztonsági szintjét és az alkalmazandó biztonsági funkciókat, pl.: Drive Encryption.

  MEGJEGYZÉS: A HP Client Security sok funkciója személyre szabható a HP és a biztonsági hivatalnok együttműködésével. További tudnivalók: http://www.hp.com.

- IT rendszergazda—A biztonsági hivatalnok által meghatározott biztonsági funkciókat alkalmazza és kezeli. Néhány funkciót engedélyezhet vagy le is tilthat. Például, ha a biztonsági hivatalnok az intelligens kártyák használata mellett döntött, az IT rendszergazda engedélyezheti a jelszó és intelligens kártya módját is.

- Felhasználó—Használják a biztonsági funkciókat. Például, ha a biztonsági hivatalnok éa az IT rendszergazda engedélyezte az intelligens kártyák használatát a rendszerhez, akkor a felhasználó beállíthatja az intelligens kártya PIN-kódját, és használhatja a kártyát a hitelesítéshez.

VIGYÁZAT! A rendszergazdákat arra bátorítjuk, hogy kövessék a végfelhasználó privilégiumainak korlátozására és a felhasználói hozzáférések korlátozására vonatkozó "legjobb gyakorlatokat".

Engedéllyel nem rendelkező felhasználóknak nem adhatók rendszergazdai privilégiumok.

A HP Client Security Manager jelszavainak kezelése

A HP Client Securitylegtöbb funkcióját jelszó biztosítja. Az alábbi táblázat felsorolja a szokásosan használt jelszavakat, a szoftvermodulokat, ahol a jelszót beállították, és a jelszó funkcióját.

A jelszavakat csak az IT rendszergazdát állítják be és használják, és ebben a táblázatban is szerepelnek. Minden más jelszót szokásos felhasználók vagy rendszergazdák is beállíthatnak.

HP Client Security jelszava	Beállítás az alábbi modulban	Funkció
Windows-bejelentkezési jelszó	Windows vezérlőpult vagy HP Client Security	Manuális bejelentkezéshez és a különböző HP Client Security funkciókhoz való hozzáférés hitelesítéséhez használható.
HP Client Security biztonsági mentés és helyreállítási jelszava	HP Client Security, egyéni felhasználóval	Védi a HP Client Security biztonsági mentés és helyreállítási fájljához való hozzáférést.
Intelligenskártya PIN-kódja	Credential Manager	Többtényezős hitelesítésként használható. Windows hitelesítésként használható. Hitelesíti a Drive Encryption felhasználóját, ha az intelligens kártya van kiválasztva.

Biztonságos jelszó létrehozása

Jelszavak létrehozásánáál először a program által beállított specifikációkat kell követni. Általában azonban fontolja meg az alábbi irányelveket, hogy segítsenek erős jelszavakat létrehozni, és csökkentsék a jelszó kompromittálásának esélyét:

- 6 karakternél, sőt lehetőleg 8 karakternél hosszabb jelszót használjon.
- Keverje a jelszóban a kis- és nagybetűáket.
- Hacsak lehetséges, keverje az alfanumerikus karaktereket és tegyen bele speciális karaktereket és írásjeleket.
- Helyettesítse a speciális karaktereket vagy számokat betűkkel egy kulcsszóban. Például használhatja az 1-es számot az I vagy L betűkhöz.
- 2 vagy több nyelvből kombináljon szavakat.
- Hasítsa szét a szót vagy kifejezést számokkal vagy speciális karakterekkel középen, például: “Mary2-2Cat45.”
- Ne használjon olyan jelszót, mely szótárban megtalálható.
- Ne használja jelszóként a nevét vagy más személyes adatokat, például a születési dátumát, kedvence nevét vagy anyja leánykori nevét, még visszafelé leírva se!
- Rendszeresen módosítsa a jelszavát. Csak néhány karaktert elég megváltoztatnia.
- Ha leírja a jelszavát, ne tárolja könnyen látható helyen, nagyon közel a számítógéphez.
- Ne mentse el a jelszavát fájlba, például e-mailben, a számítógépen.
- Ne ossza meg senkivel a fiókjait és ne mondja el a jelszavait.

A biztonsági mentés hitelesítő adatai és beállításai

Használhatja a HP Client Security biztonsági mentés és helyreállítás eszközét központi helyként, ahol elvégezheti a biztonsági hitelesítő adatok biztonsági mentését és helyreállítását néhány telepített HP Client Security modulból.

2 Első lépések

A HP Client Security hitelesítő adataival való használatához konfigurálásához indítsa el a HP Client Security programot az alábbi módok egyikével. Amint befejezte a felhasználó a varázslót, az a felhasználó nem indíthatja el ismét.

1. A kezdő- vagy alkalmazások képernyőn kattintson vagy koppintson a **HP Client Security** alkalmazásra (Windows 8).

   – vagy –

   A Windows asztalon kattintson vagy koppintson a **HP Client Security** eszközre (Windows 7).

   – vagy –

   A Windows asztalon kétszer kattintson vagy duplán koppintson a **HP Client Security** ikonra az értesítési területen, mely a feladatsor jobb oldalán található.

   – vagy –

   A Windows asztalon kattintson vagy koppintson a **HP Client Security** ikonra az értesítési területen, majd válassza a **HP Client Security megnyitása** elemet.

2. A HP Client Security telepítő varázslója a megjelenített üdvözlőképernyővel indul.

3. Olvassa el az üdvözlőképernyőt, igazolja a személyazonosságát a Windows jelszava begépelésével, majd kattintson vagy koppintson a **Tovább** lehetőségre.

   Ha még nem hozott létre Windows jelszót, a rendszer felszólítja rá. A Windows jelszó azért szükséges, hogy megvédje a Windows fiókját az illetéktelen személyek hozzáférésétől, és hogy használhassa a HP Client Security funkciókat.

4. A HP SpareKey oldalon válasszon három biztonsági kérdést. Adjon választ mindegyik kérdésre, majd kattintson a **Tovább** gombra. A szokásos kérdések is engedélyezettek. További információ itt olvasható: HP SpareKey—Jelszó helyreállítása, 15. oldal.

5. Az ujjlenyomat oldalon regisztrálja legalább a minimális számú szükséges ujjlenyomatot, majd kattintson vagy koppintson a **Tovább** gombra. További információ itt olvasható: Ujjlenyomatok, 13. oldal.

6. A Drive Encryption oldalon aktiválja a titkosítást, készítsen biztonsági másolatot a titkosítási kulcsról, majd kattintson vagy koppintson a **Tovább** gombra. További információ: a HP Drive Encryption szoftver súgója.

MEGJEGYZÉS: Ez arra a forgatókönyvre vonatkozik, ahol a felhasználó rendszergazda, és a HP Client Security telepítő varázslót korábban rendszergazda nem konfigurálta.

7. A varázsló utolsó oldalán kattintson vagy koppintson a **Befejezés** gombra.

   Ez az oldal megadja a funkciók és hitelesítő adatok állapotát.

8. A HP Client Security telepítő varázslója bizosítja a Pont időben hitelesítés és a File Sanitizer funkcióinak aktiválását. További információ: HP eszközhozzáférés-kezelő szoftver súgója és a HP File Sanitizer szoftver súgója.

MEGJEGYZÉS: Ez arra a forgatókönyvre vonatkozik, ahol a felhasználó rendszergazda, és a HP Client Security telepítő varázslót korábban rendszergazda nem konfigurálta.

A HP Client Security megnyitása

A következő módok egyikével nyithatja meg a HP Client Security alkalmazást:

MEGJEGYZÉS: A HP Client Security telepítő varázslóját be kell fejezni mielőtt a HP Client Security alkalmazás elindítható.

- A kezdő- vagy alkalmazások képernyőn kattintson vagy koppintson a **HP Client Security** alkalmazásra.

  – vagy –

  A Windows asztalon kattintson vagy koppintson a **HP Client Security** eszközre (Windows 7).

  – vagy –

  A Windows asztalon kétszer kattintson vagy duplán koppintson a **HP Client Security** ikonra az értesítési területen, mely a feladatsor jobb oldalán található.

  – vagy –

  A Windows asztalon kattintson vagy koppintson a **HP Client Security** ikonra az értesítési területen, majd válassza a **HP Client Security megnyitása** elemet.

3 Easy Setup Guide kis üzleteknek

Ennek a fejezetnek a célja az alap lépések bemutatása a HP Client Security for Small Business leggyakoribb és leghasznosabb opciónak aktiválásához. Ebben a szoftverben számos eszköz és opció teszi lehetővé, hogy finoman beállítsa a preferenciáit és a hozzáférés szabályozását. Jelen Easy Setup Guide középpontjában az áll, hogy mindegyik futó modult megkapja a legkisebb beállítási próbával és idővel. További információkért válassza ki azt a modult, amely érdekli, majd kattintson a **?** Súgó gombra a jobb felső sarokban. Ez a gomb automatikusan megjeleníti azon információkat, melyek segítenek a jelenleg megjelenített ablakkal.

Első lépések

1. A Windows asztalon kétszer kattintson a **HP Client Security** ikonra az értesítési területen, mely a feladatsor jobb oldalán található, hogy megnyissa a HP Clietn Security alkalmazást.
2. Adja meg a Windows jelszavéát, vagy hozzon létre egy Windows jelszót.
3. Végezze el a HP Client Security beállítását.

Hogy a HP Client Security rendelkezésre álljon, csak egyszer kell hitelesíteni a Windows bejelentkezés során, lásd: Biztonsági funkciók, 28. oldal.

Password Manager

Mindenkinek sok jelszava van, különösen, ha rendszeresen hozzáfér olyan weboldalakhoz vagy használ olyan alkalmazásokat, melyekhez be kell jelentkeznie. A normál felhasználó vagy ugyanazt a jelszót használja minden alkalmazáshoz és weboldalhoz, vagy kreatív lesz és azonnal elfelejti, melyik jelszó, melyik alkalmazáshoz tartozik.

A Password Manager automatikusan emlékszik a jelszavaira, vagy hagyja megkülönböztetni, hogy mely helyekre emlékezzen és melyeket hagyjon ki. Amint bejelentkezik a számítógépre, a Password Manager megadja a jelszavakat vagy hitelesítő adatokat az alkalmazásokhoz vagy weboldalakhoz.

Amikor hozzáfér valamilyen alkalmazáshoz vagy weboldalhoz, melyhez hitelesítő adatokra van szükség, a Password Manager automatikusn felismeri a helyet, és megkérdezi, hogy szeretné-e, hogy a szoftver emlékezzen az információkra. Ha szeretne bizonyos oldalakat kizárni, akkor tagadja meg a kérést

A webhelyek, felhasználónevek és jelszavak mentésének elkezdéséhez:

1. Példaként menjen egy résztvevő weboldalra vagy alkalmazáshoz, majd kattintson a Password Manager ikonra a weboldal bal felső sarkában, hogy hozzáadja a webes hitelesítést.
2. Nevezze meg a hivatkozást (opcionális) és adjon meg egy felhasználónevet és jelszót a Password Manager-ben.
3. Amikor készen van, kattintson az **OK** gombra.
4. A Password Manager el tudja menteni a felhasználóneveit és jelszavait hálózati megosztásokhoz vagy feltérképezett hálózati meghajtókhoz is.

A mentett hitelesítések megtekintése és kezelése a Password Manager-ben

A Password Manager lehetővé teszi, hogy egy központi helyről a hitelesítéseit megtekintse, kezelje, arról biztonsági mentést készítsen és azt elindítsa. A Password Manager támogatja a mentett helyek elindítását is a Windows-ból.

A Password Manager megnyitásához használja a Ctrl+Windows billentyű+h billentyűkombinációt, majd kattintson a **Bejelentkezés** opcióra a mentett parancsikon elindítására és hitelesítésére.

A Password Manager **Szerkesztés** opciója lehetővé teszi, hogy megtekintse és módosítsa a nevet, a bejelentkezési nevet sőt akár felfedje a jelszavakat.

A HP Client Security for Small Business lehetővé teszi az összes hitelesítő adat és beállítás biztonsági mentését és/vagy másolását másik számítógépre.

HP eszközhozzáférés-kezelő

A Device Access Manager segítségével korlátozható különböző belső és külső tárolóeszközök használata, így az adatok biztonságban maradnak a merevlemezen és nem jutnak ki vállalkozása ajtaján. Például lehetővé teszi, hogy egy felhasználó hozzáférjen az adataihoz, de nem engedi, hogy CD-re, személyes zenelejátszóra vagy USB memóriaeszközre másolja azokat.

1. Nyissa meg a **Device Access Manager** alkalmazást (lásd: Az eszközhozzáférés-kezelő megnyitása, 44. oldal).

   Az aktuális felhasználók hozzáférései megjelennek.

2. A felhasználók, csoportok vagy eszközök hozzáférésének megváltoztatásához kattintson vagy érintse meg a **Módosítás** opciót. További információ itt olvasható: Rendszernézet, 45. oldal.

HP Drive Encryption

A HP Drive Encryption segítségével a teljes merevlemez titkosításával védheti meg az adatait. A merevlemezén található adatok védettek maradnak, ha bármikor ellopják a számítógépét és/vagy ha a merevlemezt kiveszik ez eredeti számítógépből és másik gépbe teszik be.

További biztonsági előny at, hogy a Drive Encryption elvárja Öntől, hogy megfelően hitelesítse a felhasználónevét és jelszavát az operációs rendszer elindulása előtt. Ezt a folyamatot hívják bootloás előtti hitelesítésnek.

Hogy könnyű legyen, több szoftvermodul szinkronizálja automatikusan a jelszavakat, beleértve a Windows felhasználói fiókokat, a hitelesítő doméneket, a HP Drive Encryption-t, a Password Manager-t és a HP Client Security-t.

A HP Drive Encryption beállításához az első telepítéskor a HP Client Security Setup varázslóval lásd: Első lépések, 9. oldal.

4 HP Client Security

A HP Client Security kezdőlapja a HP Client Security funkciók, alkalmazások és beállítások könnyű hozzáféréséhez központi helyen van. A kezdőlap három részre osztódik:

- **ADATOK**—Hozzáférést biztosít az adatok biztonságát felhasználó alkalmazásokhoz.
- **ESZKÖZ**—Hozzáférést biztosít az eszköz biztonságát felhasználó alkalmazásokhoz.
- **SZEMÉLYAZONOSSÁG**—A hitelesítő adatok regisztrálását és kezelését biztosítja.

Vigye a kurzort egy alkalmazás ikonja fölé, hogy megjelenjen az alkalmazás leírása.

A HP Client Security hivatkozásokat ad meg a felhasználónak és rendszergazdai beállításokat az oldal alján. A HP Client Security hozzáférést nyújt a Haladó beállításokhoz és funkciókhoz, ha a **Fogaskerék** (beállítások) ikonra koppint vagy kattint.

Személyazonossággal kapcsolatos funkciók, alkalmazások és beállítások

A HP Client Security által biztosított személyazonossággal kapcsolatos funkciók, alkalmazások és beállítások segítik Önt a digitális személyazonosság különféle szempontjainak kezelésében. Kattintson vagy koppintson az alábbi ikonok egyikére a HP Client Security kezdőlapján, majd adja meg a Windows jelszavát.

- **Ujjlenyomatok**—Regisztrálja és kezeli az ujjlenyomat hitelesítő adatait.
- **SpareKey**—Telepíti és kezeli a HP SpareKey hitelesítő adatait, melyek a számítógépre bejelentkezéshez használhatók, ha az egyéb hitelesítő adatok elvesztek vagy rosszak. Az elfelejtett jelszó visszaállítását is lehetővé teszi.
- **Windows jelszó**—Könnyű hozzáférést biztosít a Windows jelszó módosításához.
- **Bluetooth eszközök**—Lehetővé teszi a Bluetooth eszközei regisztrálását és kezelését.
- **Kártyák**—Lehetővé teszi, hogy az intelligens kártyáit, érintkezés nélküli kártyáit és közelségérzékelő kártyáit regisztrálja és kezelje.
- **PIN-kód**—Lehetővé teszi a PIN-kódos hitelesítő adatok regisztrálását és kezelését.
- **RSA SecurID**—Lehetővé teszi az RSA SecurID hitelesítő adatai regisztrálását és kezelését (ha megfelelő telepítés van).
- **Password Manager**—Lehetővé teszi online fiókjai és alkalmazásai jelszavainak kezelését.

Ujjlenyomatok

A HP Client Security telepítő varázsló végigvezeti Önt a telepítési vagy ujjlenyomatának "regisztrálási" folyamatán.

Az Ujjlenyomatok oldalon regisztrálhatja vagy törölheti is az ujjlenyomatait. Ehhez az **Ujjlenyomatok** ikonra kattintva fér hozzá a HP Client Security kezdőlapján.

1. Az Ujjlenyomatok oldalon húzza el az ujját, amíg sikeresen regisztrálásra nem kerül.

   A regisztrálni szükséges ujjak száma az oldalon látható. A legjobb a mutató- vagy középsőujj.

2. Korábban regisztrált ujjlenyomatok törléséhez kattintson vagy koppintson a **Törlés** gombra.
3. További ujjak regisztrálásához kattintson vagy koppintson a **További ujjlenyomat regisztrálása** pontra.
4. Kattintson vagy koppintson a **Mentés** gombra, mielőtt elhagyja az oldalt.

⚠ **VIGYÁZAT!** Amikor ujjlenyomatokat regisztrál a varázsló segítségével, akkor az ujjlenyomat adatai nem kerülnek mentésre, csak amikor a **Tovább** gombra kattint. Ha egy időre a számítógép inaktív lesz vagy bezárja a programot, akkor az elvégzett módosítások **nem** kerülnek mentésre.

- Az ujjlenyomatok rendszergazdai beállításainak eléréséhez kattintson vagy koppintson a **Rendszergazdai beállítások** elemre (ehhez rendszergazdai jogosultságok szükségesek). Itt a rendszergazdák meghatározhatják a regisztrálást, a pontosságot és más beállításokat.
- Az Ujjlenyomat felhasználói beállítások hozzáféréséhez kattintson vagy koppintson a **Felhasználói beállítások** elemre. Itt meghatározhatja az ujjlenyomat-felismerés megjelenését és viselkedését irányító beállításokat.

Ujjlenyomatok rendszergazdai beállításai

A rendszergazda határozza meg a regisztrálást, a pontosságot és az ujjlenyomat-olvasó egyéb beállításait. Rendszergazdai jogosultságok szükségesek.

- Az ujjlenyomatos hitelesítő adatok rendszergazdai beállításainak eléréséhez kattintson vagy koppintson az Ujjelnyomatok oldalon a **Rendszergazdai beállítások** elemre.

- **Felhasználó regisztrálása**—Válassza ki azt a minimális és maximális számú ujjlenyomatot, melyet egy felhasználó regisztrálhat.
- **Felismerés**—A csúszka mozgatásával állítsa be az ujjlenyomat-olvasó által alkalmazott érzékenységet, amikor az ujját lehúzza.

  Ha következetesen nem ismeri fel az ujjlenyomatát, akkor lehet, hogy alacsonyabb felismerési beállítást kell választania. A magasabb beállítás növeli az ujjlenyomatok lehúzásánál a variációk érzékenységét, és ezért csökkenti a hamis elfogadás lehetőségét. A **Közepes** beállítás jó keverékét adja a biztonságnak és a kényelemnek.

Ujjlenyomatok felhasználói beállításai

Az Ujjlenyomat felhasználói beállítások oldalon meghatározhatja azon beállításokat, melyek az ujjlenyomat-felismerés megjelenését és viselkedését irányítják.

▲ Az ujjlenyomatos hitelesítő adatok Felhasználói beállításainak eléréséhez kattintson vagy koppintson az Ujjlenyomatok oldalon a **Felhasználói beállítások** elemre.

- **Hangos visszajelzés engedélyezése**—Alapértelmezésként a HP Client Security hangos visszajelzés ad, amikor egy ujjlenyomatot lehúznak, és az adott programeseményekhez különböző hangokat játszik le. Kijelölhet új hangokat ezekhez az eseményekhez a Hangok lapon a hangbeállítások menüben a Windows vezérlőpulton, vagy letilthatja a hangos visszajelzést a jelölőnégyzet törlésével.
- **A beolvasási minőség visszajelzésének megmutatása**—Jelölje ki a jelölőnégyzetet az összes lehúzás megjelenítéséhez a minőségtől függetlenül. Csak a jó minőségű lehúzások megjelenítéséhez törölje a jelölőnégyzetet.

HP SpareKey—Jelszó helyreállítása

A HP SpareKey lehetővé teszi, hogy hozzáférést nyerjen a számítógépéhez (támogatott platformokon) három biztonsági kérdésre válaszolva.

A HP Client Security megkéri Önt, hogy állítsa be a személyes HP SpareKey adatait az első telepítés alatt a HP Client Security telepítő varázslójában.

A HP SpareKey telepítéséhez:

1. A varázsló HP SpareKey oldalán válasszon három biztonsági kérdést, majd adja meg mindegyik kérdésre a választ.

   Választhat kérdést az előre meghatározott listáról vagy írhat saját kérdést is.

2. Kattintson vagy koppintson a **Regisztrálás** gombra.

A HP SpareKey törléséhez:

▲ Kattintson vagy koppintson a **SpareKey törlése** gombra.

A SpareKey telepítése után hozzáférhet a számítógépéhez a SpareKey segítségével a rendszerindításkori hitelesítés bejelentkező képernyőn vagy a Windows üdvözlőképernyőn.

Választhat más kérdéseket vagy módosíthatja a válaszait a SpareKey oldalon, melyet a jelszó helyreállítása ikonról érhet el a HP Client Security kezdőlapon.

A HP SpareKey beállításainak eléréséhez kattintson a **Beállítások** elemre (rendszergazdai jogosultságokat igényel). Itt a rendszergazda meghatározhatja a HP SpareKey hitelesítő adatokra vonatkozó beállításokat.

HP SpareKey Settings

A HP SpareKey beállítások oldalon meghatározhatja azon beállítéásokat, melyek a HP SpareKey hitelesítő adatok viselkedését és használatát irányítják.

▲ A HP SpareKey beállítások oldal elindításához kattintson vagy koppintson a HP SpareKey oldalon a **Beállítások** elemre (rendszergazdai jogosultságokat igényel).

A rendszergazdák az alábbi beállításokat választhatják ki:

- Határozza meg a kérdéseket, melyek megjelennek majd minden felhasználónak a HP SpareKey telepítése közben.
- Legfeljebb három szokásos kérdést adjon hozzá a felhasználóknak mutatott listához.
- Válassza ki, hogy a felhasználók írhatnak-e saját biztonsági kérdéseket vagy sem.
- Határozza meg, milyen hitelesítési környezet (Windows vagy rendszerindításkori hitelesítés) teszi lehetővé a HP SpareKey használatát a jelszó helyreállításához.

Windows-jelszó

A HP Client Security a Windows jelszavát egyszerűbben és gyorsabban megváltoztatja, mint a Windows vezérlőpult.

A Windows jelszó módosításához:

1. A HP Client Security kezdőlapon kattintson vagy koppintson a **Windows jelszó** elemre.
2. Adja meg a jelenlegi jelszavát a **Jelenlegi Windows jelszó** szövegmezőben.
3. Gépeljen be új jelszót az **Új Windows jelszó** szövegmezőbe, majd gépelje be ismét az **Új jelszó megerősítése** szövegmezőbe.
4. A jelenlegi jelszó azonnal megváltoztatásához az újonnan megadottra kattintson vagy koppintson a **Módosítás** gombra.

Bluetooth-eszközök

Ha a rendszergazda engedélyezte a Bluetooth-t hitelesítő adatként, akkor beállíthat egy Bluetooth-os telefont más hitelesítő adatokkal együtt a további biztonság érdekében.

MEGJEGYZÉS: Csak a Bluetooth-os telefonok támogatottak.

1. Győződjön meg arról, hogy a Bluetooth engedélyezve van a számítógépen és hogy a Bluetooth-os telefon felfedezhető módban van. A telefonhoz csatlakozáshoz szükség lehet egy automatikusn generált kód begépelésére a Bluetooth-eszközön. A Bluetooth-eszköz konfigurációs beállításaitól függően a párodsító kódok összehasonlítása a számítógép és a telefon között szükséges lehet.
2. A telefon regisztrálásához válassza ki, majd kattintson vagy koppintson a **Regisztrálás** pontra.

A Bluetooth-eszközök beállításai, 16. oldal oldal eléréséhez kattintson a **Beállítások** elemre (rendszergazdai jogosultságokat igényel). Itt a rendszergazda meghatározhatja a Bluetooth-eszközök beállításait.

Bluetooth-eszközök beállításai

A rendszergazdák az alábbi beállításokat határozhatják meg, melyek a Bluetooth-eszköz hitelesítő adatainak viselkedését és használatát irányítják:

Csendes hitelesítés

- **Automatikusan használja a csatlakoztatott, regisztrált Bluetooth-eszközét a személyazonossága igazolása közben**—Jelölje ki a jelölőnégyzetet, hogy a felhasználók használhassák a Bluetooth-os hitelesítő adatokat a hitelesítéshez anélkül, hogy a felhasználónak tennie kellene valamit, vagy törölje a jelölőnégyzetet az opció letiltásához.

Bluetooth közelsége

- **Zárolja a számítógépet, amikor a regisztrált Bluetooth-eszköze kikerül a számítógép tartományából**—Jelölje ki a jelölőnégyzetet a számítógép zárolásához, amikor a bejelentkezés alatt csatlakoztatott Bluetooth-eszköz kikerül a tartományból, vagy törölje a jelölőnégyzetet az opció letiltásához.

MEGJEGYZÉS: A számítógépén a Bluetooth-moduljának támogatnia kell ezt a képességet, hogy élvezhesse e funkció előnyeit.

Kártyák

A HP Client Security támogathat sok, különféle típusú azonosítókártyát, melyek kis műanyag, számítógép-chipet tartalmazó kártyák. Ide tartoznak az intelligens kártyák, az érintkezés nélküli kártyák és a közelségérzékelő kártyák. Ha ezen kártyák egyike és a megfelelő kártyaolvasó csatlakozik a számítógéphez, ha a rendszergazda telepítette a gyártótól kapott, hozzá tartozó meghajtót, és ha a rendszergazda engedélyezte a kártyát hitelesítő adatként, akkor használhatja a kártyát hitelesítő adatként.

Az intelligens kártyák esetében a gyártónak kell biztosítani az eszközöket egy biztonsági igazolás és PIN-kód telepítésének kezeléséhez, melyet a HP Client Security használ a biztonsági algoritmusában. A PIN-kódként használatos karakterek száma és típusa változhat. Rendszergazdának kell inicializálnia az intelligens kártyát, mielőtt használni lehet.

A HP Client Security az alábbi intelligenskártya-formátumokat támogatja:

- CSP
- PKCS11

A HP Client Security az alábbi érintkezésnélkülikártya-formátumokat támogatja:

- Érintkezés nélküli HID iCLASS memóriakártyák
- Érintkezés nélküli MiFare Classic 1k, 4k és mini memóriakártyák

A HP Client Security az alábbi közelségérzékelőkártya-formátumokat támogatja:

- HID közelségérzékelő kártya

Intelligens kártya regisztrálásához:

1. Helyezze be a kártyát a mellékelt intelligenskártya-olvasóba.
2. Amikor felismeri a kártyát, adja meg a kártya PIN-kódját, majd kattintson vagy koppintson a **Regisztrálás** gombra.

Az intelligens kártya PIN-kódjának módosításához:

1. Helyezze be a kártyát a mellékelt intelligenskártya-olvasóba.
2. Amikor felismeri a kártyát, adja meg a kártya PIN-kódját, majd kattintson vagy koppintson a **Hitelesítés** gombra.
3. Kattintson vagy koppintson a **PIN-kód módosítása** elemre, majd adja meg az új PIN-kódot.

Érintkezés nélküli vagy közelségérzékelő kártya regisztrálásához:

1. Tegye a kártyát a megfelelő olvasóra vagy ahhoz nagyon közel.
2. Amikor a kártyát felismeri, kattintson vagy koppintson a **Regisztrálás** gombra.

Regisztrált kártya törlése:

1. Tegye a kártyát a kártyaolvasóhoz.
2. Csak az intelligens kártyák esetén adja meg a kártya kijelölt PIN-kódját, majd kattintson vagy koppintson a **Hitelesítés** gombra.
3. Kattintson vagy koppintson a **Törlés** gombra.

Amint megtörtént a kártya regisztrálása, megjelennek a kártya adatai a **Regisztrált kártyák** pont alatt. Amikor töröl egy kártyát, eltűnik a listáról.

A közelségérzékelő, érintkezés nélküli és intelligens kártya beállításainak eléréséhez kattintson vagy koppintson a **Beállítások** pontra (rendszergazdai jogosultságokat igényel). Itt a rendszergazdák meghatározhatják a kártya hitelesítő adataira vonatkozó beállításokat.

Közelségérzékelő, érintkezés nélküli és intelligens kártyák beállításai

Egy kártya beállításainak eléréséhez kattintson vagy koppintson a kártyára a listában, majd kattintson vagy koppintson a megjelenő nyílra.

Az intelligens kártya PIN-kódjának módosításához:

1. Tegye a kártyát az olvasóhoz.
2. Adja meg a kártya kijelölt PIN-kódját, majd kattintson vagy koppintson a **Folytatás** gombra.
3. Adja meg és erősítse meg az új PIN-kódot, majd kattintson vagy koppintson a **Folytatás** gombra.

Az intelligens kártya PIN-kódjának inicializálásához:

1. Tegye a kártyát az olvasóhoz.
2. Adja meg a kártya kijelölt PIN-kódját, majd kattintson vagy koppintson a **Folytatás** gombra.
3. Adja meg és erősítse meg az új PIN-kódot, majd kattintson vagy koppintson a **Folytatás** gombra.
4. Kattintson vagy koppintson az **Igen** lehetőségre az inicializálás megerősítéséhez.

A kártyaadatok törléséhez:

1. Tegye a kártyát az olvasóhoz.
2. Adja meg a kártya kijelölt PIN-kódját (csak intelligens kártya esetén), majd kattintson vagy koppintson a **Folytatás** gombra.
3. Kattintson vagy koppintson az **Igen** lehetőségre a törlés megerősítéséhez.

PIN-kód

Ha a rendszergazda engedélyezte a PIN-kódot hitelesítő adatként, akkor beállíthat egy PIN-kódot más hitelesítő adatokkal együtt a további biztonság érdekében.

Új PIN-kód beállításához:

- Adja meg a PIN-kódot, adja meg újra a megerősítéshez, majd kattintson vagy koppintson az **Alkalmaz** pontra.

PIN-kód törléséhez:

- Kattintson vagy koppintson a **Törlés** pontra, majd kattintson vagy koppintson az **Igen** lehetőségre.

A PIN-kód beállításainak eléréséhez kattintson vagy koppintson a **Beállítások** pontra (rendszergazdai jogosultságokat igényel). Itt a rendszergazdák meghatározhatják a PIN-kód hitelesítő adataira vonatkozó beállításokat.

PIN beállítások

A PIN-kód beállításai oldalon meghatározhatja a PIN-kód hitelesítő adat minimálisan és maximálisan elfogadható hosszát.

RSA SecurID

Ha a rendszergazda engedélyezte az RSA-t hitelesítő adatként, és a következő feltételek igazak, akkor regisztrálhat vagy törölhet RSA SecurID hitelesítő adatot.

MEGJEGYZÉS: Megfelelő telepítés szükséges.

- A felhasználót létre kell hozni egy RSA kiszolgálón.
- A felhasználóhoz kijelölt RSA SecurID tokent és a számítógépet csatlakoztatni kell az RSA kiszolgáló doménjéhez.
- A SecurID szoftver telepítve van a számítógépen.
- A megfelelően konfigurált RSA kiszolgálóhoz elérhető a csatlakozás.

RSA SecurID hitelesítő adat regisztrálásához:

▲ Adja meg az RSA SecurID felhasználónevét és jelszavát (RSA SecurID token kódja vagy PIN-kód + token kód a környezettől függően), majd kattintson vagy koppintson az **Alkalmaz** elemre.

Sikeres regisztráláskor megjelenik egy üzenet: "Az RSA SecurID hitelesítő adata sikeresen regisztrálásra került", és engedélyezésre kerül a Törlés gomb.

RSA SecurID hitelesítő adat törléséhez:

▲ Kattintson a **Törlés** pontra, majd válassza az **Igen** lehetőséget a felugró ablakban, amelyben azt kérdezik: "Biztosan törölni szeretné az RSA SecurID hitelesítő adatot?"

Password Manager

A weboldalakra és az alkalmazásokba a bejelentkezés könnyebb és biztonságosabb a Password Manager használatával. Erősebb jelszavakat is létrehozhat, melyeket nem kell leírnia vagy megjegyeznie, majd könnyen és gyorsan bejelentkezhet ujjlenyomattal, intelligens kártyával, közelségérzékelő kártyával, érintkezés nélküli kártyával, Bluetooth-telefonnal, PIN-kóddal, RSA hitelesítő adattal vagy a Windows jelszavával.

MEGJEGYZÉS: A webes bejelentkező képernyők állandó változása miatt a Password Manager lehet, hogy nem minden weboldalt és nem mindig támogat.

A Password Manager az alábbi lehetőségeket nyújtja:

Password Manager oldal

- Kattintson vagy koppintson egy fiókra, hogy automatikusan elindítson egy weboldalt vagy alkalmazást, és bejelentkezzen.
- Használjon kategóriákat a fiókjai rendezéséhez.

Jelszó erőssége

- Gyorsan nézze meg, hogy valamelyik jelszava biztonsági kockázat-e.
- Bejelentkezési adatok hozzáadásakor ellenőrizze a weboldalakhoz és alkalmazásokhoz használt adott jelszó erősségét.
- A jelszó erősségét piros, sárga vagy zöld állapotjelző illusztrálja.

A weboldal vagy alkalmazás bejelentkezési képernyőjének bal felső sarkában jelenik meg a **Password Manager**. Amikor még nem hozott létre bejelentkezést ahhoz a weboldalhoz vagy alkalmazáshoz, akkor az ikonon megjelenik egy plusz jel.

▲ Kattintson vagy koppintson a **Password Manager** ikonra, hogy helyi menü jelenjen meg, ahol az alábbi opciókból választhat:

- [somedomain.com] hozzáadása a Password Manager-hez
- Password Manager megnyitása
- Ikonbeállítások
- Súgó

Olyan weboldalak vagy programok esetén, ahol még nem hozott létre bejelentkezést

Az alábbi opciók jelennek meg a helyi menüben:

- **[somedomain.com] hozzáadása a Password Manager-hez**—Lehetővé teszi, hogy bejelentkezést adjon hozzá a jelenlegi bejelentkezési képernyőhöz.
- **Password Manager megnyitása**—Elindítja a Password Manager-t.
- **Ikonbeállítások**—Lehetővé teszi, hogy olyan feltételeket határozzon meg, amelyben megjelenik a **Password Manager** ikon.
- **Súgó**—Megjeleníti a HP Client Security súgóját.

Olyan weboldalak vagy programok esetén, ahol már létrehozott bejelentkezést

Az alábbi opciók jelennek meg a helyi menüben:

- **Bejelentkezési adatok kitöltése**—Megjeleníti a **Személyazonosság igazolása** oldalt. Ha sikeresen hitelesítette, akkor a bejelentkezési adatai bekerülnek a bejelentkezési mezőkbe, majd az oldal elküldésre kerül (ha meghatározták a küldést, amikor bejelentkezést hoztak létre vagy szerkesztettek legutóbb).
- **Bejelentkezés szerkesztése**—Lehetővé teszi, hogy szerkessze e weboldaal bejelentkezési adatait.
- **Bejelentkezés hozzáadása**—Lehetővé teszi, hogy fiókot adjon a Password Manager-hez.
- **Password Manager megnyitása**—Elindítja a Password Manager-t.
- **Súgó**—Megjeleníti a HP Client Security súgóját.

MEGJEGYZÉS: E számítógép rendszergazdája lehet, hogy konfigurálta a HP Client Security szofvert, hogy egy vagy több hitelesítő adatot kérjen a személyazonosság igazolásakor.

Bejelentkezések hozzáadása

Könnyen hozzáadhat bejelentkezési adatokat weboldalakhoz vagy programhoz az adatok egyszeri megadásával. Onnantól a Password Manager automatikusan megadja Önnek az adatokat. Ezeket a bejelentkezési adatokat a weboldal vagy program böngészése után is használhatja.

Bejelentkezés hozzáadásához:

1. Nyissa meg a weboldal vagy program bejelentkezési képernyőjét.
2. Kattintson vagy koppintson a **Password Manager** ikonra, majd kattintson vagy koppintson az alábbiak egyikére attól függően, hogy weboldal vagy program bejelentkezési képernyője:
   - Weboldalak esetén kattintson vagy koppintson a **[domain name] hozzáadása a Password Manager-hez** elemre.
   - Program esetén kattintson vagy koppintson a **Bejelentkezési képernyő hozzáadása a Password Manager-hez** elemre.
3. Adja meg bejelentkezési adatait. A képernyőn a bejelentkezési mezőket és a párbeszédablakban a megfelelő mezőket vastagított, narancssárga határ azonosítja.
   a. A bejelentkezési mező kitöltéséhez az egyik előre formázott választással kattintson vagy koppintson a mező jobb oldalán található nyilakra.
   b. A bejelentkezéshez tartozó jelszó megtekintéséhez kattintson vagy koppintson a **Jelszó mutatása** elemre.
   c. A bejelentkezési mezők kitöltetéséhez, de nem elküldéséhez törölje a **Bejelentkezési adatok automatikus elküldése** jelölőnégyzetet.
   d. Kattintson vagy koppintson az **OK**-ra a használni kívánt hitelesítési mód (ujjlenyomat, intelligens kártya, közelségérzékelő kártya, érintkezés nélküli kártya, Bluetooth-telefon, PIN-kód vagy jelszó) kiválasztásához, majd jelentkezzen be a kiválasztott hitelesítési móddal.

      A plusz jel eltűnik a **Password Manager** ikonról, ezzel értsítve, hogy a bejelentkezés elkészült.
   e. Ha a Password Manager nem észleli a bejelentkezési mezőket, akkor kattintson vagy koppintson a **További mezők** elemre.
      - Jelölje be a bejelentkezéshez szükséges jelölőnégyzeteket, vagy törölje azoknak a mezőknek a jelölését, amelyek nem szükségesek a bejelentkezéshez.
      - Kattintson vagy koppintson a **Bezárás** gombra.

Minden alkalommal, amikor eléri azt a weboldalt vagy megnyitja a programot, a weboldal vagy alkalmazás bejelentkezési képernyőjének bal felső sarkában megjelenik a **Password Manager** ikon. Ezzel jelzi, hogy a bejelentkezéshez használhatja a regisztrált hitelesítő adatait.

Bejelentkezések szerkesztése

Bejelentkezés szerkesztéséhez:

1. Nyissa meg a weboldal vagy program bejelentkezési képernyőjét.
2. Olyan párbeszédablak megjelenítéséhez, ahol szerkesztheti a bejelentkezési adatait, kattintson vagy koppintson a **Password Manager** ikonra, majd kattintson vagy koppintson a **Bejelentkezés szerkesztése** elemre.

   A képernyőn a bejelentkezési mezőket és a párbeszédablakban a megfelelő mezőket vastagított, narancssárga határ azonosítja.

   Szerkesztheti a fiókadatokat a Password Manager oldalról is, ha a bejelentkezésre kattint vagy koppint a szerkesztési lehetőségek megjelenítéséhez, majd kiválasztja a **Szerkesztés** elemet.
3. Szerkessze a bejelentkezési adatait.
   - A **Fióknév** szerkesztéséhez adjon meg új nevet a mezőben.
   - **Kategória** nevének hozzáadásához vagy szerkesztéséhez adja meg vagy módosítsa a nevet a **Kategória** mezőben.
   - A **Felhasználói név** bejelentkezési mező kiválasztásához az egyik előre formázott választással kattintson vagy koppintson a mező jobb oldalán található lefelé nyílra.

     Az előre formázott választások csak akkor érhetők el, amikor a bejelentkezést a Password Manager ikon helyi menüjének Szerkesztés parancsával szerkeszti.
   - A **Jelszó** bejelentkezési mező kiválasztásához az egyik előre formázott választással kattintson vagy koppintson a mező jobb oldalán található lefelé nyílra.

     Az előre formázott választások csak akkor érhetők el, amikor a bejelentkezést a Password Manager ikon helyi menüjének Szerkesztés parancsával szerkeszti.
   - További mezők hozzáadásához a képernyőről a bejelentkezéséhez kattintson vagy koppintson a **További mezők** lehetőségre.
   - A bejelentkezéshez tartozó jelszó megtekintéséhez kattintson vagy koppintson a **Jelszó mutatása** ikonra.
   - A bejelentkezési mezők kitöltetéséhez, de nem elküldéséhez törölje a **Bejelentkezési adatok automatikus elküldése** jelölőnégyzetet.
   - E bejelentkezés megjelöléséhez, hogy a jelszava kompromittált, jelölje ki az **Ez a jelszó kompromittált** jelölőnégyzetet.

     A módosítások mentése után az összes egyéb, azonos jelszavú bejelentkezés is kompromittáltként lesz megjelölve. Ezutánb meglátogathatja ,indegyik érintett fiókot, és szükség szerint módosíthatja a jelszavakat.
4. Kattintson vagy koppintson az **OK** gombra.

A Password Manager gyorshivatkozások menü használata

A Password Manager gyors, könnyű módot biztosít az olyan weboldalak és programok elindításához, melyekhez hozott létre bejelentkezést. Kétszer kattintson vagy duplán koppintson egy program vagy weboldal bejelentkezésére a **Password Manager gyorshivatkozások** menüben vagy a Password Manager oldalon, a HP Client Security programon belül, hogy megnyissa a bejelentkezési képernyőt, majd kitöltse a bejelentkezési adatokat.

Amikor bejelentkezést hoz létre, automatikusan hozzáadásra kerül a Password Manager **gyorshivatkozások** menüjéhez.

A **gyorshivatkozások** menü megjelenítéséhez:

▲ Nyomja le a **Password Manager** alkalmazáshoz tartalmazó gyorsbillentyű-kombinációt ((Ctrl +Windows billentyű+h a gyári beállítás). A gyorsbillentyű-kombináció módosításához a HP Client Security kezdőlapján kattintson a **Password Manager** ikonra, majd kattintson vagy koppintson a **Beállítások** elemre.

A bejelentkezések kategóriába rendezése

Hozzon létre egy vagy több kategóriát, hogy sorban maradjanak a bejelentkezései.

Bejelentkezés kategóriához jelöléséhez:

1. A HP Client Security kezdőlapon kattintson vagy koppintson a **Password Manager** elemre.
2. Kattintson vagy koppintson a fiók bevitelére, majd kattintson vagy koppintson az **Szerkesztés** gombra.
3. A **Kategória** mezőben adjon meg egy kategórianevet.
4. Kattintson vagy koppintson a **Mentés** gombra.

Fiók eltávolításához egy kategóriából:

1. A HP Client Security kezdőlapon kattintson vagy koppintson a **Password Manager** elemre.
2. Kattintson vagy koppintson a fiók bevitelére, majd kattintson vagy koppintson az **Szerkesztés** gombra.
3. A **Kategória** mezőben törölje a kategórianevet.
4. Kattintson vagy koppintson a **Mentés** gombra.

Kategória átnevezéséhez:

1. A HP Client Security kezdőlapon kattintson vagy koppintson a **Password Manager** elemre.
2. Kattintson vagy koppintson a fiók bevitelére, majd kattintson vagy koppintson az **Szerkesztés** gombra.
3. A **Kategória** mezőben módosítsa a kategórianevet.
4. Kattintson vagy koppintson a **Mentés** gombra.

Bejelentkezések kezelése

A Password Manager megkönnyíti a bejelentkezési adatai kezelését felhasználónevek, jelszavak és több bejelentkezési fiók esetén, egy központi helyről.

A bejelentkezései a Password Manager oldalon vannak felsorolva.

A bejelentkezései kezeléséhez:

1. A HP Client Security kezdőlapon kattintson vagy koppintson a **Password Manager** elemre.
2. Kattintson vagy koppintson egy létező bejelentkezésre, majd válasszon egyet az alábbi lehetőségek közül, majd kövesse a képernyőn megjelenő utasításokat:
   - **Szerkesztés**—Bejelentkezés szerkesztése. További információ itt olvasható: Bejelentkezések szerkesztése, 22. oldal.
   - **Bejelentkezés**—Bejelentkezés a kiválasztott fiókba.
   - **Törlés**—A kiválasztott fiók bejelentkezésének törlése.

További bejelentkezés hozzáadása weboldalhoz vagy programhoz:

1. Nyissa meg a weboldal vagy program bejelentkezési képernyőjét.
2. Kattintson vagy koppintson a **Password Manager** ikonra, hogy megjelenjen a helyi menüje.
3. Kattintson a **Bejelentkezés hozzáadása** gombra, majd kövesse a képernyőn megjelenő utasításokat.

Jelszava erősségének értékelése

Személyazonosságának védelme szempontjából fontos, hogy erős jelszavakat használjon a weboldalakra és programokba történő bejelentkezéshez.

A Password Manager a weboldalaira és programjaiba való bejelentkezéshez használt jelszavai erősségének azonnali és automatikusa elemzésével könnyen figyeli és javítja a biztonságot.

Amikor egy fiókhoz Password Manager bejelentkezést hoz létre és jelszót ad meg, egy színes sáv jelzi a jelszó erősségét a jelszó alatt. A színek az alábbi értékeket jelzik:

- **Piros**—gyenge
- **Sárga**—közepes
- **Zöld**—erős

A Password Manager ikon beállításai

A Password Manager megpróbálja azonosítani a weboldalak és programok bejelentkezési képernyőit. Ha olyan bejelentkezési képernyőt észlel, melyhez még nem hozott létre bejelentkezést, akkor a Password Manager megkéri Önt, hogy adjon bejelentkezést a képernyőhöz a **Password Manager** ikont plusz jellel megjelenítve.

1. Kattintson vagy koppintson az ikonra, majd kattintson vagy koppintson az **Ikon beállításai** elemre, hogy testre szabja, hogy a Password Manager hogyan kezelje a lehetséges bejelentkezési helyeket.
   - **Kérés a bejelentkezési képernyőkhöz bejelentkezések hozzáadására**—Kattintson vagy koppintson erre a lehetőségre, hogy a Password Manager megkérje Önt, hogy bejelentkezést adjon hozzá, amikor bejelentkezési képernyő jelenik meg, amelyhez még nincs bejelentkezés telepítve.
   - **A képernyő kizárása**—Jelölje ki a jelölőnégyzetet, hogy a Password Manager ne kérje meg ismét bejelentkezés hozzáadására ehhez a bejelentkezési képernyőhöz.
   - **Ne kérje a bejelentkezési adatok hozzáadását a bejelentkezési képernyőkhöz**—Állítsa be a választógombot.
2. Bejelentkezés hozzáadásához egy képernyőhöz, melyet korábban kizárt:
   a. Jelentkezzen be a korábban kizárt weboldalra.
   b. Hogy a Password Manager emlékezzen az oldal jelszavára, kattintson vagy koppintson a felugró párbeszédablakban az **Emlékezz** pontra, hogy elmentse a jelszót, és bejelentkezést hozzon létre a képernyőhöz.
3. További Password Manager beállítások eléréséhez kattintson vagy koppintson a Password Manager ikonra, kattintson vagy koppintson a **Password Manager megnyitása**, majd a **Beállítások** pontra a Password Manager oldalon.

Bejelentkezések importálása és exportálása

A HP Password Manager Importálás és exportálás oldalon importálhatja a webböngészők által a számítógépen elmentett bejelentkezéseket. Importálhat adatokat egy HP Client Security biztonságimásolat-fájlból is, és exportálhat adatokat egy HP Client Security biztonságimásolat-fájlba is.

- ▲ Az Importálás és exportálás oldal elindításához kattintson vagy koppintson a Password Manager oldalon az **Importálás és exportálás** pontra.

Jelszavak importálásához böngészőből:

1. Kattintson vagy koppintson arra a böngészőre, ahonnak importálni szeretné a jelszavakat (csak a telepített böngészők jelennek meg).
2. Törölje a jelölőnégyzetét minden fióknak, melyhez nem szeretne jelszavakat importálni.
3. Kattintson vagy koppintson az **Importálás** gombra.

Adatok importálása innen, vagy adatok exportálása ide, HP Client Security biztonságimásolat-fájl készíthető a kapcsolódó hivatkozásokon (az **Egyéb lehetőségek** pont alatt) az Importálás és exportálás oldalon.

MEGJEGYZÉS: Ez a funkciócsak a Password Manager adatokat importálja és exportálja. További HP Client Security adatok biztonsági mentéséről és visszaállításáról további információk: Biztonsági mentés és adatai visszaállítása, 29. oldal.

Adatok importálásához HP Client Security biztonságimásolat-fájlból:

1. A HP Password Manager Importálás és exportálás oldalán kattintson vagy koppintson az **Adatok importálása HP Client Security biztonságimásolat-fájlból** elemre.
2. Igazolja a személyazonosságát.
3. Válassza ki a korábban létrehozott biztonságimásolat-fájlt vagy adja meg az elérési útját a megadott mezőben, majd kattintson vagy koppintson a **Böngészés** pontra.
4. Adja meg a fájl védelmére használt jelszót, majd kattintson vagy koppintson a **Tovább** gombra.
5. Kattintson vagy koppintson az **Visszaállítás** gombra.

Adatok exportálásához HP Client Security biztonságimásolat-fájlba:

1. A HP Password Manager Importálás és exportálás oldalán kattintson vagy koppintson az **Adatok exportálása HP Client Security biztonságimásolat-fájlba** elemre.
2. Igazolja a személyazonosságát, majd kattintson vagy koppintson a **Tovább** pontra.
3. Adjon nevet a biztonságimásolat-fájlnak. Alapértelmezés szerint a fájl a Dokumentumok mappában kerül mentésre. Más hely meghatározásához kattintson vagy koppintson a **Böngészés** gombra.
4. Adja meg és erősítse meg a fájl védelmére használt jelszót, majd kattintson vagy koppintson a **Mentés** gombra.

Beállítások

Meghatározhatja a beállításokat a Password Manager személyre szabásához:

- **Kérés bejelentkezések hozzáadására bejelentkezési képernyőkhöz**—Megjelenik a **Password Manager** ikon egy plusz jellel, ahol weboldal vagy program bejelentkezést észlel a rendszer. Ezzel jelzi, hogy hozzáadhat bejelentkezést ehhez a képernyőhöz a **Bejelentkezések** menühöz.

  E funkció letiltásához törölje a jelölőnégyzetet a **Kérés bejelentkezések hozzáadására bejelentkezési képernyőkhöz** alatt.

- **Password Manager megnyitása a Ctrl+Win+h kombinációval**—Az alapértelmezett gyorsbillentyű, mely megnyitja a **Password Manager gyorhivatkozások** menüt: Ctrl+Windows billentyű+h.

  A gyorsbillentyű módosításához kattintson vagy koppintson erre a pontra, majd adjon meg új billentyűkombinációt. Az alábbiak közül egyet vagy többet tartalmazhatnak a kombinációk: ctrl, alt vagyshift és bármilyen betű- vagy számbillentyű

  Nem használhatók a Windows vagy Windows alkalmazások számára fenntartott kombinációk.

- A beállítások gyári beállításokra történő visszaállításához kattintson vagy koppintson az **Alapértelmezett visszaállítása** pontra.

Speciális beállítások

A rendszergazdák hozzáférhetnek az alábbi opciókhoz, ha kiválasztják a **fogaskerék** (beállítások) ikont a HP Client Security kezdőképernyőjént.

- **Rendszergazdai szabályok**—Lehetővé teszi, hogy bejelentkezési és munkamenet szabályokat konfiguráljon a rendszergazdáknak.
- **Szokásos felhasználói szabályok**—Lehetővé teszi, hogy bejelentkezési és munkamenet szabályokat konfiguráljon a szokásos felhasználóknak.
- **Biztonsági szolgáltatások**—Lehetővé teszi számítógépe biztonságának növelését a Windows fiók védelmével, erős hitelesítés alkalmazásával és/vagy a hitelesítés engedélyezésével a Windows indítása előtt.
- **Felhasználók**—Lehetővé teszi felhasználók és hitelesítő adataik kezelését.
- **Irányelveim**—Lehetővé teszi, hogy átnézze a hitelesítési házirendjét és a regisztrálási állapotát.
- **Biztonsági mentés és visszaállítás**—Lehetővé teszi a HP Client Security adatainak biztonsági mentését és visszaállítását.
- **A HP Client Security névjegye**—Megjeleníti a HP Client Security verzióadatait.

Rendszergazdák házirendje

Bejelentkezési és munkamenet szabályokat konfigurálhat a számítógép rendszergazdáinak. Az itt beállított bejelentkezési szabályok irányítják egy helyi rendszergazdának szükséges hitelesítő adatokat a Windows-ba való bejelentkezéshez. Az itt beállított munkamenet szabályok irányítják egy helyi rendszergazdának szükséges hitelesítő adatokat Windows munkamenetben a személyazonosság igazolásához.

Alapértelmezés szerint az összes új vagy módosított szabály azonnal hatályba lép az **Alkalmaz** gombra koppintva vagy kattintva.

Új szabály hozzáadásához:

1. A HP Client Security kezdőlapon kattintson vagy koppintson a **Fogaskerék** ikonra.
2. A Speciális beállítások oldalon kattintson vagy koppintson a **Rendszergazdai házirend** elemre.
3. Kattintson vagy koppintson az **Új szabály hozzáadása** pontra.
4. Kattintson a lefelé nyílra, hogy kiválassza az elsődleges és (opcionális) másodlagos hitelesítő adatokat az új szabályhoz, majd kattintson vagy koppintson a **Hozzáad** gombra.
5. Kattintson az **Alkalmaz** elemre.

Új vagy módosított szabály hatályba lépésének késleltetéséhez:

1. Kattintson vagy koppintson a **Szabály azonnali hatályba lépése** elemre.
2. Válassza az **Adott napon lépjen érvénybe ez a szabály** pontot.
3. Adjon meg egy napot, vagy válasszon ki egy napot a felugró naptárban, amikor a szabálynak hatályba kell lépnie.
4. Ha kívánja, válassza ki, mikor emlékeztesse a felhasználókat az új szabályra.
5. Kattintson az **Alkalmaz** elemre.

Standard felhasználói házirend

Bejelentkezési és munkamenet szabályokat konfigurálhat a számítógép standard felhasználóinak. Az itt beállított bejelentkezési szabályok irányítják egy standard felhasználónak szükséges hitelesítő adatokat a Windows-ba való bejelentkezéshez. Az itt beállított munkamenet szabályok irányítják egy standard felhasználónak szükséges hitelesítő adatokat Windows munkamenetben a személyazonosság igazolásához.

Alapértelmezés szerint az összes új vagy módosított szabály azonnal hatályba lép az **Alkalmaz** gombra koppintva vagy kattintva.

Új szabály hozzáadásához:

1. A HP Client Security kezdőlapon kattintson vagy koppintson a **Fogaskerék** ikonra.
2. A Speciális beállítások oldalon kattintson vagy koppintson a **Standard felhasználói házirend** elemre.
3. Kattintson vagy koppintson az **Új szabály hozzáadása** pontra.
4. Kattintson a lefelé nyílra, hogy kiválassza az elsődleges és (opcionális) másodlagos hitelesítő adatokat az új szabályhoz, majd kattintson vagy koppintson a **Hozzáad** gombra.
5. Kattintson az **Alkalmaz** elemre.

Új vagy módosított szabály hatályba lépésének késleltetéséhez:

1. Kattintson vagy koppintson a **Szabály azonnali hatályba lépése** elemre.
2. Válassza az **Adott napon lépjen érvénybe ez a szabály** pontot.
3. Adjon meg egy napot, vagy válasszon ki egy napot a felugró naptárban, amikor a szabálynak hatályba kell lépnie.
4. Ha kívánja, válassza ki, mikor emlékeztesse a felhasználókat az új szabályra.
5. Kattintson az **Alkalmaz** elemre.

Biztonsági funkciók

Engedélyezheti a HP Client Security funkcióit, melyek segítenek megvédeni a számítógépet az illetéktelen hozzáféréstől.

A biztonsági szolgáltatások beállításához:

1. A HP Client Security kezdőlapon kattintson vagy koppintson a **Fogaskerék** ikonra.
2. A Speciális beállítások oldalon kattintson vagy koppintson a **Biztonsági szolgáltatások** elemre.
3. Engedélyezze a biztonsági szolgáltatásokat a jelölőnégyzetek kijelölésével, majd kattintson vagy koppintson az **Alkalmaz** gombra. Minél több funkciót választ ki, annál biztonságosabb lesz a számítógépe.

   Ezek a beállítások minden felhasználóra vonatkoznak.

   - **Windows bejelentkezési biztonság**—Védi a Windows fiókjait, mivel a hozzáféréshez a HP Client Security hitelesítő adatokat igényli.
   - **Rendszerindítás előtti biztonság (rendszerindításkori hitelesítés)**—Védi a számítógépép a Windows elindítása előtt. Ez a választás nem érhető el, ha a BIOS nem támogatja.
   - **Egylépéses bejelentkezés engedélyezése**—Ez a beállítás lehetővé teszi, hogy átugorja a Windows bejelentkezést, ha a rendszerindításkori hitelesítéskor vagy a Drive Encryption szinten korábban elvégezte a hitelesítést.
4. Kattintson vagy koppintson a **Felhasználók** pontra, majd kattintson vagy koppintson a felhasználó ikonjára.

Felhasználók

Figyelheti és kezelheti a számítógép HP Client Security felhasználóit.

Egy másik Windows felhasználó hozzáadásához a HP Client Security-hez:

1. A HP Client Security kezdőlapon kattintson vagy koppintson a **Fogaskerék** ikonra.
2. A Speciális beállítások oldalon kattintson vagy koppintson a **Felhasználók** elemre.
3. Kattintson vagy koppintson az **Egy másik Windows felhasználó hozzáadása a HP Client Security-hez** elemre.
4. Adja meg a hozzáadni kívánt felhaszn-ló nevét, majd kattintson vagy koppintson az **OK** gombra.
5. Adja meg a felhasználó Windows-jelszavát.

   A Felhasználó oldalon megjelenik egy ikon a hozzáadott felhasználó esetén.

Windows felhasználó törléséhez a HP Client Security-ből:

1. A HP Client Security kezdőlapon kattintson vagy koppintson a **Fogaskerék** ikonra.
2. A Speciális beállítások oldalon kattintson vagy koppintson a **Felhasználók** elemre.
3. Kattintson vagy koppintson a törölni kívánt felhasználó nevére.
4. Kattintson vagy koppintson a **Felhasználó törlése** pontra, majd a megerősítéshez kattintson vagy koppintson az **Igen** lehetőségre.

A felhasználókra érvényes bejelentkezési és munkamenet szabályok összefoglalásának megjelenítéséhez:

▲ Kattintson vagy koppintson a **Felhasználók** pontra, majd kattintson vagy koppintson a felhasználó ikonjára.

Irányelveim

Megjelenítheti a hitelesítési házirendjét és a regisztrálási állapotát. Az Irányelveim oldal hivatkozásokkal is szolgál a Rendszergazdai és Standard felhasználói házirend oldalaihoz.

1. A HP Client Security kezdőlapon kattintson vagy koppintson a **Fogaskerék** ikonra.
2. A Speciális beállítások oldalon kattintson vagy koppintson az **Irányelveim** elemre.

   Megjelennek az éppen bejelentkezett felhasználóra érvényes bejelentkezési és munkamenet szabályok.

Az Irányelveim oldal hivatkozásokkal is szolgál a Rendszergazdák házirendje, 26. oldal és Standard felhasználói házirend, 27. oldal pontokhoz.

Biztonsági mentés és adatai visszaállítása

Javasolt, hogy rendszeresen biztonsági másolatot készítsen a HP Client Security adatairól. Hogy milyen gyakran készítsen biztonsági másolatot, az az adatok módosításának gyakoriságától függ. Például ha minden nap új bejelentkezéseket ad hozzá, akkor naponta kell biztonsági másolatot készítenie az adatairól.

A biztonsági másolatok használhatók egyik számítógépről a másikra vitelre is, melynek neve importálás és exportálás.

MEGJEGYZÉS: Ezzel a funkcióval csak a Password Manager-ről készül biztonsági másolat. A Drive Encryption független biztonsági mentési móddal rendelkezik. Az eszközhozzáférés-kezelő és az ujjlenyomatos hitelesítés adatairól nem készül biztonsági másolat.

A HP Client Security programot minden számítógépre telepíteni kell, hogy megkapja a biztonsági másolat adatait, mielőtt az adatok visszaállíthatók a biztonságimásolat-fájlból.

Adatai biztonsági mentéséhez:

1. A HP Client Security kezdőlapon kattintson vagy koppintson a **Fogaskerék** ikonra.
2. A Speciális beállítások oldalon kattintson vagy koppintson a **Rendszergazdai házirend** elemre.
3. Kattintson vagy koppintson a **Biztonsági mentés és visszaállítás** gombra.
4. Kattintson vagy koppintson a **Biztonsági mentés** gombra, majd azonosítsa a személyazonosságát.
5. Válassza ki azt a modult, melyet bele szeretne tenni a biztonsági mentésbe, majd kattintson vagy koppintson a **Tovább** elemre.
6. Adjon nevet a tárolófájlnak. Alapértelmezés szerint a fájl a Dokumentumok mappában kerül mentésre. Más hely meghatározásához kattintson vagy koppintson a **Böngészés** gombra.
7. Adjon meg és erősítse meg egy jelszót a fájl védelmére.
8. Kattintson vagy koppintson a **Mentés** gombra.

Adatok visszaállításához:

1. A HP Client Security kezdőlapon kattintson vagy koppintson a **Fogaskerék** ikonra.
2. A Speciális beállítások oldalon kattintson vagy koppintson a **Rendszergazdai házirend** elemre.
3. Kattintson vagy koppintson a **Biztonsági mentés és visszaállítás** gombra.
4. Válassza a **Visszaállítás** gombot, majd azonosítsa a személyazonosságát.
5. Válassza ki a korábban létrehozott tárolófájlt. Adja meg az elérési utat a megadott négyzetben. Más hely meghatározásához kattintson vagy koppintson a **Böngészés** gombra.
6. Adja meg a fájl védelmére használt jelszót, majd kattintson vagy koppintson a **Tovább** gombra.
7. Válassza ki azt a modult, ahová vissza szeretné állítani az adatokat.
8. Kattintson vagy koppintson az **Visszaállítás** gombra.

5 HP Drive Encryption (csak bizonyos modelleknél)

A HP Drive Encryption teljes adatvédelmet kínál a számítógépe adatainak titkosításával. A Drive Encryption bekapcsolt állapotában be kell jelentkeznie a Drive Encryption bejelentkező képernyőjén, amely még a Windows® operációs rendszer betöltése előtt megjelenik.

A HP Client Security kezdőlap lehetővé teszi, hogy a Windows rendszergazdák aktiválják a Drive Encryption-t, a titkosítási kulcs biztonsági mentését, illetve kijelöljék vagy megszüntessék a meghajtó(k) vagy partíció(k) kijelölését a titkosításhoz. További információ: a HP Client Security szoftver súgója.

Az alábbi feladatok végezhetők el a Drive Encryption szoftverrel:

- A Drive Encryption beállításainak kiválasztása:
  - Egyedi meghajtók vagy partíciók titkosítása vagy visszafejtése szoftvertitkosítás segítségével
  - Egyedi öntitkosító meghajtók titkosítása vagy visszafejtése hardvertitkosítás segítségével
  - További biztonság hozzáadása az Alvó vagy Készenléti üzemmód letiltásával annak biztosítása érdekében, hogy a Drive Encryption rendszerindítás előtti hitelesítése mindig szükséges legyen

MEGJEGYZÉS: Kizárólag a belső SATA és külső eSATA-merevlemezek titkosíthatók.

- Biztonsági mentési kulcsok készítése
- Hozzáférés helyreállítása egy titkosított számítógéphez biztonsági mentési kulcsok és HP SpareKey segítségével
- A Drive Encryption rendszerindítás előtti hitelesítésének engedélyezése jelszó, regisztrált ujjlenyomat vagy választott intelligens kártyákhoz való PIN-kód használatával

A Drive Encryption megnyitása

A rendszergazdák hozzáférhetnek a Drive Encryption szoftverhez a HP Client Security megnyitásával:

1. A kezdőképernyőn kattintson vagy koppintson a **HP Client Security** alkalmazásra (Windows 8).

   – vagy –

   A Windows asztalon kétszer kattintson vagy duplán koppintson a **HP Client Security** ikonra az értesítési területen, mely a feladatsor jobb oldalán található.

2. Kattintson vagy koppintson a **Drive Encryption** ikonra.

Általános feladatok

A Drive Encryption aktiválása szokásos merevlemezekhez

A szokásos merevlemezek szoftvertitkosítással kerülnek titkosításra. Kövesse ezen lépéseket egy meghajtó vagy lemezpartíció titkosításához:

1. Indítsa el a **Drive Encryption** alkalmazást. További információ itt olvasható: A Drive Encryption megnyitása, 31. oldal.
2. Jelölje ki a titkosítani kívánt meghajtó vagy partíció jelölőnégyzetét, majd kattintson vagy koppintson a **Biztonsági mentési kulcs** elemre.

MEGJEGYZÉS: A jobb biztonság érdekében jelölje ki a **Alvó üzemmód letiltása a jobb biztonsághoz** jelölőnégyzetet. Amikor letiltja az alvó üzemmódot, akkor abszolút nem áll fenn annak a kockázata, hogy a meghajtó zárolásának feloldásához használt hitelesítő adatok tárolásra kerüljenek a memóriában.

3. Válasszon egy vagy több biztonsági mentési opciót, majd kattintson vagy koppintson a **Biztonsági mentés** elemre. További információ itt olvasható: Titkosítási kulcsok biztonsági mentése, 35. oldal.
4. A titkosítási kulcs biztonsági mentése közben folytathatja a munkát. Ne indítsa újra a számítógépet.

MEGJEGYZÉS: A rendszer kéri majd a számítógép újraindítását. Az újraindítás után megjelenik a Drive Encryption rendszerindítás előtti képernyője, mely hitelesítést igényel a Windows elindulása előtt.

A Drive Encryption aktivált. A kiválasztott meghajtópartíció(k) titkosítása akár több óráig is eltarthat a partíció(k) számától és méretétől függően.

További információ: a HP Client Security szoftver súgója.

A Drive Encryption aktiválása öntitkosító meghajtók esetén

Az öntitkosító meghajtók kezelésére vonatkozó Trusted Computing Group OPAL jellemzőjének megfelelő öntitkosító meghajtók szoftver- vagy hardvertitkosítással titkosíthatók. A hardvertitkosítás sokkal gyorsabb, mint a szoftvertitkosítás. Viszont nem választhatja ki, hogy melyik lemezpartíciót titkosítja. Az egész lemez, beleértve az összes lemezpartíciót, titkosításra kerül.

Adott partíciók titkosításához tehát a szoftvertitkosítást kell használnia. Győződjön meg arról, hogy törölje a **Kizárólag a hardvertitkosítás engedélyezése az öntitkosító meghajtók (SED) esetén** jelölőnégyzetet.

Kövesse az alábbi lépéseket a Drive Encryption aktiválásához öntitkosító meghajtók esetén:

1. Indítsa el a **Drive Encryption** szoftvert. További információ itt olvasható: A Drive Encryption megnyitása, 31. oldal.
2. Jelölje ki a titkosítani kívánt meghajtó jelölőnégyzetét, majd kattintson vagy koppintson a **Biztonsági mentési kulcs** elemre.

MEGJEGYZÉS: A jobb biztonság érdekében jelölje ki a **Alvó üzemmód letiltása a jobb biztonsághoz** jelölőnégyzetet. Amikor letiltja az alvó üzemmódot, akkor abszolút nem áll fenn annak a kockázata, hogy a meghajtó zárolásának feloldásához használt hitelesítő adatok tárolásra kerüljenek a memóriában.

3. Válasszon egy vagy több biztonsági mentési opciót, majd kattintson vagy koppintson a **Biztonsági mentés** elemre. További információ itt olvasható: Titkosítási kulcsok biztonsági mentése, 35. oldal.

4. A titkosítási kulcs biztonsági mentése közben folytathatja a munkát. Ne indítsa újra a számítógépet.

MEGJEGYZÉS: Az öntitkosító meghajtók esetén megkéri majd a rendszer a számítógép leállítására.

További információ: a HP Client Security szoftver súgója.

A Drive Encryption inaktiválása

1. Indítsa el a **Drive Encryption** szoftvert. További információ itt olvasható: A Drive Encryption megnyitása, 31. oldal.

2. Törölje az összes titkosított meghajtó jelölőnégyzetét, majd kattintson vagy koppintson az **Alkalmaz** gombra.

   Elkezdődik a Drive Encryption inaktiválása.

MEGJEGYZÉS: Ha szoftvertitkosítást használt, elkezdődik a visszafejtés. Több óráig is eltarthat a titkosított merevlemez-partíció(k) méretétől függően. Amikor készen van a visszafejtés, a Drive Encryption inaktivált.

Ha hardvertitkosítást használt, a meghajtó azonnal visszafejtésre kerül, és néhány perc után a Drive Encryption inaktivált.

Amint inaktivált a Drive Encryption, megkéri majd a rendszer, hogy állítsa le a számítógépet, ha hardvertitkosított, vagy indítsa újra a számítógépet, ha szoftvertitkosított.

Bejelentkezés a Drive Encryption aktiválása után

Amikor, a Drive Encryption aktiválása után bekapcsolja a számítógépet, és a felhasználói fiókja regisztrált, akkor a Drive Encryption bejelentkezési képernyőn be kell jelentkeznie:

MEGJEGYZÉS: Amikor Alvó vagy Készenléti üzemmódból tér magához a számítógép, a Drive Encryption rendszerindítás előtti hitelesítése nem jelenik meg a szoftvertitkosítás vagy hardvertitkosítás esetén. A hardvertitkosítás biztosítja az **Alvó üzemmód letiltása a jobb biztonság érdekében** lehetőséget, mely megakadályozza az Alvó vagy Készenléti üzemmódba kerülést, amikor engedélyezett.

Amikor Hibernált üzemmódból tér magához a számítógép, a Drive Encryption rendszerindítás előtti hitelesítése megjelenik a szoftvertitkosítás vagy hardvertitkosítás esetén egyaránt.

MEGJEGYZÉS: Ha a Windows rendszergazda engedélyezte a BIOS rendszerindítás előtti biztonságot a HP Client Security programban, és ha az egylépéses bejelentkezés engedélyezett (alapértelmezésként), akkor bejelentkezhet a számítógépre rögtön a hitelesítés után a BIOS rendszerindítás előtt anélkül, hogy újra kellene hitelesíteni a Drive Encryption bejelentkezési képernyőjén.

Egyfelhasználós bejelentkezés:

- A **Bejelentkezés** oldalon adja meg a Windows jelszavát, az intelligens kártya PIN-kódját, a SpareKey-t vagy húzza le az egyik regisztrált ujját.

Többfelhasználós bejelentkezés:

1. A **Felhasználó kiválasztása a bejelentkezéshez** oldalon válassza ki a legördülő listából a bejelentkezni kívánó felhasznbálót, majd kattintson vagy koppintson a **Tovább** pontra.
2. A **Bejelentkezés** oldalon adja meg a Windows jelszavát, az intelligens kártya PIN-kódját vagy húzza le az egyik regisztrált ujját.

MEGJEGYZÉS: Az alábbi intelligens kártyák támogatottak:

Támogatott intelligens kártyák

- Gemalto Cyberflex Access 64k V2c

MEGJEGYZÉS: Ha a Drive Encryption bejelentkezési képernyőn helyreállító kulcsot használ a bejelentkezéshez, akkor további hitelesítő adatok szükségesek a Windows bejelentkezéskor a felhasználói fiókok eléréséhez.

További merevlemezek titkosítása

Nagyon javasolt, hogy használja a HP Drive Encryption programot adatai védelmére, a merevlemez titkosításával. Aktiválás után minden hozzáadott merevlemez vagy létrehozott partíció az alábbi lépésekkel titkosítható:

1. Indítsa el a **Drive Encryption** szoftvert. További információ itt olvasható: A Drive Encryption megnyitása, 31. oldal.
2. A szoftvertitkosított meghajtók esetén válassza ki a titkosítandó meghajtópartíciókat.

MEGJEGYZÉS: Ez vonatkozik egy vegyes meghajtó forgatókönyvre is, ahol egy vagy több szokásos merevlemez és egy vagy több öntitkosító meghajtó van.

– vagy –

▲ A hardvertitkosított meghajtók esetén válassza ki a titkosítandó kiegészítő meghajtó(ka)t.

Haladó feladatok

Drive Encryption kezelése (rendszergazdai feladat)

A rendszergazdák használhatják a Drive Encryption szoftvert a számítógépen található összes merevlemezt titkosítási állapotának (titkosított vagy nem titkosított) megtekintésére és módosítására.

- Ha az állapot engedélyezett, akkor a Drive Encryption aktivált és konfigurált. A meghajtó az alábbi állapotok egyikében van:

Szoftvertitkosítás

- Nem titkosított
- Titkosított
- Titkosítás
- Visszafejtés

Hardvertitkosítás

- Titkosított
- Nem titkosított (további meghajtók esetén)

Egyedi meghajtópartíciók titkosítása vagy visszafejtése (csak szoftvertitkosítás)

A rendszergazdák a Drive Encryption szoftverrel egy vagy több merevlemez-partíciót titkosíthatnak a számítógépen, vagy visszafejthetnek bármilyen meghajtó-partíciót, melyet már titkosítottak.

1. Indítsa el a **Drive Encryption** szoftvert. További információ itt olvasható: A Drive Encryption megnyitása, 31. oldal.
2. A **Meghajtó állapota** menüben jelölje ki vagy törölje az adott, titkosítani vagy visszafejteni szándékozott merevlemez-partíció melletti jelölőnégyzetet, majd kattintson vagy koppintson az **Alkalmaz** gombra.

MEGJEGYZÉS: Amikor partíciót titkosít vagy fejt vissza, egy haladást jelző sávon megjelenik a titkosított partíció százaléka.

MEGJEGYZÉS: A dinamikus partíciók nem támogatottak. Ha egy partíció csak úgy megjelenik, de nem titkosítható, amikor kiválasztja, akkor a partíció dinamikus. Dinamikus partíció egy partíció zsugorításakor jön létre, hogy a Lemezkarbantartáson belül új partíciót hozzon létre.

Figyelmeztetés jelenik meg, ha egy partíció dinamikus partícióvá alakul át.

Lemezkarbantartás

- **Becenév**—A könnyebb azonosításhoz nevet adhat a meghajtóinak vagy partícióinak.
- **Lecsatlakoztatott meghajtók**—A Drive Encryption nyomon követheti a számítógépről eltávolított lemezeket. A számítógépről eltávolított lemezek automatikusan a Lecsatlakoztatott listába kerülnek. Ha a lemez visszakerül a rendszerbe, ismét megjelenik a Csatlakoztatott listában.
- Ha tovább már nem kell követni vagy kezelni a lecsatlakoztatott meghajtót, akkor az eltávolítható a Lecsatlakoztatott listából.
- A Drive Encryption aktivált marad, amíg az összes csatlakoztatott meghajtó jelölőnégyzete törlésre nem kerül, és a Lecsatlakoztatott lista üres nem lesz.

Biztonsági mentés és helyreállítás (rendszergazdai feladat)

Amikor a Drive Encryption aktivált, a rendszergazdák használhatják a titkosítási kulcs biztonsági mentése oldalt a titkosítási kulcsok biztonsági mentésére cserélhető adathordozóra, és helyreállítás végrehajtására.

Titkosítási kulcsok biztonsági mentése

A rendszergazdák biztonsági mentést készíthetnek egy titkosított meghajtó titkosítási kulcsáról cserélhető tárolóeszközre.

VIGYÁZAT! GFyőződjön meg arról, hogy a biztonsági mentési kulcsot tartalmazó tárolóeszközt biztonságos helyen tartsa, mivel ha elfelejti a jelszavát, elveszíti az intelligens kártyáját vagy nincs regisztrált ujja, akkor ez az eszköz jelent egyetlen hozzáférést a számítógéphez. Ennek a tárolási helynek biztonságosnak is kell lennie, mivel a tárolóeszköz hozzáférést tesz lehetővé a Windowshoz.

1. Indítsa el a **Drive Encryption** szoftvert. További információ itt olvasható: A Drive Encryption megnyitása, 31. oldal.
2. Jelölje ki egy meghajtó jelölőnégyzetét, majd kattintson vagy koppintson a **Biztonsági mentési kulcs** pontra.
3. A **HP Drive Encryption helyreállító kulcs létrehozása** pontban válasszon egyet vagy többet az alábbi opciókból:
   - **Cserélhető adattároló**—Jelölje ki a jelölőnégyzetet, majd válassza ki azt a tárolóeszközt, ahová a titkosítási kulcsot menteni fogja.
   - **SkyDrive**—Jelölje be a jelölőnégyzetet. Csatlakozva kell lennie az Internetre. Jelentkezzen be a Microsoft SkyDrive-ba, majd kattintson vagy koppintson az **Igen** lehetőségre.

     MEGJEGYZÉS: A SkyDrive-on tárolt HP Drive Encryption biztonsági mentési kulcs használatához le kell azt töltenie a SkyDrive-ról egy cserélhető tárolóeszközre, majd a tárolóeszközt be kell helyeznie ebbe a számítógépbe.
   - **TPM** (csak kiválasztott modellek)—Lehetővé teszi adatai helyreállítását a TPM jelszava segítségével.

     VIGYÁZAT! Ha törölt a TPM vagy a számítógép sérült, akkor elveszíti a hozzáférését a biztonsági mentéshez. Ha ezt a módszert választja, akkor ki kell választani egy másik biztonsági mentési módszert is.
4. Kattintson vagy koppintson a **Biztonsági mentés** gombra.

   A titkosítási kulcs a kiválasztott tárolóeszközön mentésre kerül.

Hozzáférés helyreállítása egy aktivált számítógéphez biztonsági mentési kulcsok segítségével

A rendszergazdák hajthatnak végre helyreálíítást a Drive Encryption biztonsági mentési kulccsal cserélhető tárolóeszközre az aktiváláskor vagy a Drive Encryption **Biztonsági mentési kulcs** opcióját kiválasztva.

1. Helyezze be a biztonsági mentési kulcsot trartalmazó cserélhető tárolóeszközt.
2. Kapcsolja be a számítógépet.
3. Amikor megnyílik a HP Drive Encryption bejelentkezési párbeszédablak, akkor kattintson vagy koppintson a **Helyreállítás** pontra.
4. Adja meg a biztonsági mentési kulcsot tartalmazó fájl elérési útját vagy nevét, majd kattintson vagy koppintson a **Helyreállítás** gombra.
5. Amikor megnyílik a megerősítő párbeszédablak, akkor kattintson vagy koppintson az **OK**-ra.

   Megjelenik a Windows bejelentkezési képernyő.

MEGJEGYZÉS: Ha a Drive Encryption bejelentkezési képernyőn helyreállító kulcsot használ a bejelentkezéshez, akkor további hitelesítő adatok szükségesek a Windows bejelentkezéskor a felhasználói fiókok eléréséhez. Nagyon javasolt a jelszavát visszaállítani helyreállítás végrehajtása után.

HP SpareKey helyreállítás végzése

A SpareKey helyreállításhoz a Drive Encryption rendszerindítása előtt szükség van biztonsági kérdések helyes megválaszolására, mielőtt hozzáfér a számítógéphez. További információ a SpareKey helyreállítás üzembe helyezéséről: a HP Client Security szoftver súgója.

HP SpareKey helyreállítás elvégzéséhez, ha elfelejti a jelszavát:

1. Kapcsolja be a számítógépet.
2. Amikor a HP Drive Encryption oldal megjelenik, navigáljon a felhasználói bejelentkezési oldalra.
3. Kattintson az **SpareKey** gombra.

   MEGJEGYZÉS: Ha a Sparekey nem inicializált a HP Client Security programban, akkor a **SpareKey** gomb nem érhető el.

4. A megjelent kérdésekre adja meg a helyes választ, majd kattintson a **Bejelentkezés** gombra.

   Megjelenik a Windows bejelentkezési képernyő.

MEGJEGYZÉS: Ha a Drive Encryption bejelentkezési képernyőn SpareKey-t használ a bejelentkezéshez, akkor további hitelesítő adatok szükségesek a Windows bejelentkezéskor a felhasználói fiókok eléréséhez. Nagyon javasolt a jelszavát visszaállítani helyreállítás végrehajtása után.

6 HP File Sanitizer (bizonyos modellek esetén)

A File Sanitizer lehetővé teszi, hogy a számítógép belső merevlemezén biztonságosan megsemmisítse a forrásokat (például: személyes adatokat vagy fájlokat, előzmény vagy webbel kapcsolatos adatokat vagy egyéb adatkomponenseket), és időszakonként teljesen törölje a számítógép belső merevlemezét.

A File Sanitizer nem használható az alábbi típusú meghajtók teljes törlésére:

- félvezető-alapú meghajtó (SSD), beleértve a RAID-köteteket, melyek átfognak egy SSD eszközt
- USB-vel, Firewire csatlakozóval vagy eSATA interfésszel csatlakoztatott külső meghajtók

Ha megsemmisítési vagy teljes törlési műveletet próbál elvégezni egy SSD-n, akkor figyelmeztetés jelenik meg, és a művelet nem kerül elvégzésre.

Megsemmisítés

A megsemmisítés más, mint a szokásos Windows® törlési művelet. Amikor a File Sanitizer segítségével megsemmisít egy forrást, akkor a fájlok felülírásra kerülnek jelentés nélküli adatokkal, így virtuálisan lehetetlenné teszi az eredeti forrás lekérését. A Windows egyszerű törlési művelete után lehet, hogy a fájl (vagy forrás) ép marad a merev lemezen, vagy olyan állapotba kerül, ahol bírósági módszerekkel helyreállítható.

Ütemezhet későbbi megsemmisítési időpontot, vagy manuálisan aktiválhatja a megsemmisítést, ha kiválasztja a HP Client Security kezdőlapon a **File Sanitizer** ikont, vagy ha a Windows asztalon a **File Sanitizer** ikont használja. További információ: A megsemmisítés ütemezésének beállítása, 40. oldal, Jobb egérgombos kattintásos megsemmisítés, 42. oldal vagy Megsemmisítési művelet manuális kezdése, 42. oldal.

MEGJEGYZÉS: Egy .dll fájl csak akkor kerül megsemmisítésre és eltávolításra a rendszerből, ha a Lomtárba került.

Szabad lemezterület teljes törlése

Egy forrás törlése a Windows-ban nem teljesen távolítja el a forrás tartalmát a merevlemezről. A Windows csak a forrás hivatkozásait törli vagy a helyét a merevlemezen. A forrás tartalma még mindig a merevlemezen marad, amíg egy másik forrás új információval felül nem írja ugyanazt a területet a merevlemezen.

A szabad lemezterület teljes törlése lehetővé teszi, hogy biztonságosan felülírja a törölt elemet véletlen adatokkal, ezzel megakadályozva a felhasználókat, hogy a törölt elem eredeti tartalmát megtekintsék.

MEGJEGYZÉS: A szabad lemezterület teljes törlése nem biztosít további biztonságot a megsemmisített elemeknek.

Beállíthatja a szabad lemezterület teljes törlésének későbbi időpontját, vagy manuálisan aktiválhatja a korábban megsemmisített elemek szabad lemezterület teljes törlését, ha kiválasztja a HP Client Security kezdőlapon a **File Sanitizer** ikont, vagy ha a Windows asztalon a **File Sanitizer** ikont használja. További információ: A szabad lemezterület teljes törlése ütemezésének

beállítása, 41. oldal, A szabad lemezterület teljes törlésének manuális kezdése, 43. oldal vagy A File Sanitizer ikon használata, 42. oldal.

A File Sanitizer megnyitása

1. A kezdőképernyőn kattintson vagy koppintson a **HP Client Security** alkalmazásra (Windows 8).

   – vagy –

   A Windows asztalon kétszer kattintson vagy duplán koppintson a **HP Client Security** ikonra az értesítési területen, mely a feladatsor jobb oldalán található.

2. Az **Adatok** alatt kattintson vagy koppintson a **File Sanitizer** elemre.

– vagy –

▲ Kétszer kattintson vagy duplán koppintson a **File Sanitizer** ikonra a Windows asztalon.

– vagy –

▲ Jobb egérgombbal kattintson vagy koppintson, és tartsa lenyomva a **File Sanitizer** ikont a Windows asztalon, majd válassza a **File Sanitizer megnyitása** elemet.

Telepítési eljárások

Megsemmisítés—A File Sanitizer biztonságosan törli vagy semmisíti meg a kiválasztott elemkategóriákat.

1. A **Megsemmisítés** menüben jelölje ki mindegyik megsemmisítendő fájltípushoz a jelölőnégyzetet, vagy törölje a jelölőnégyzetek kijelöléseit, ha nem szeretné azokat a fájlokat megsemmisíteni.

   - **Lomtár**—Az összes Lomtárban található tételt megsemmisíti.
   - **Ideiglenes rendszerfájlok**—Megsemmisíti az összes fájlt, amely a rendszer ideiglenes mappájában található. Az alábbi környezeti változókat a következő sorrendben keresik, és az elsőnek megtalált útvonal tekintendő rendszermappának:
     - TMP
     - TEMP
   - **Ideiglenes internetes fájlok**—Megsemmisíti a weboldalak, képek és médiafájlok másolatait, melyeket a webböngésző mentett el a gyorsabb megtekintés érdekében.
   - **Cookies**—Megsemmisíti a weboldalak által, a számítógépen, – a preferenciák (például bejelentkezési adatok) mentése érdekében – elmentett összes fájlt.

2. A megsemmisítés elindításához kattintson vagy koppintson a **Megsemmisítés** elemre.

Teljes törlés—Véletlen adatokat ír a szabad területre, és megakadályozza a törölt tételek helyreállítását.

▲ A teljes törlés elindításához kattintson vagy koppintson a **Teljes törlés** elemre.

File Sanitizer opciók—Jelölje ki a jelölőnégyzetet, hogy engedélyezze az alábbi opciókat, vagy törölje a jelölőnégyzet kijelölését egy opció letiltásához:

- **Asztali ikon engedélyezése**—Megjeleníti a File Sanitizer ikont a Windows asztalán.
- **Jobb egérgombos kattintás engedélyezése**—Lehetővé teszi, hogy jobb egérgombbal kattintson vagy koppintson egy elemre, és úgy tartsa, majd kiválassza a **HP File Sanitizer – Megsemmisítés** pontot.
- **A Windows jelszó kérése a manuális megsemmisítés előtt**—Hitelesítést igényel a Windows-jelszóval egy elem manuális megsemmisítése előtt.
- **Cookies és ideiglenes internetes fájlok megsemmisítése a böngésző bezárásakor**—Az összes kiválasztott webbel kapcsolatos elemet megsemmisíti (például a böngésző URL előzményeit), amikor bezárja a webböngészőt.

A megsemmisítés ütemezésének beállítása

Ütemezhet be olyan időpontot, amikor a megsemmisítést automatikusan elvégzi a rendszer, vagy manuálisan megsemmisítheti az elemeket, bármikor. További információ: Telepítési eljárások, 39. oldal.

1. Nyissa meg a File Sanitizer-t, majd kattintson vagy koppintson a **Beállítások** pontra.
2. Későbbi időpont ütemezéséhez a kiválasztott elemek megsemmisítésére, a **Megsemmisítés ütemezése** pont alatt válassza a **Soha**, **Egyszer**, **Naponta**, **Hetente** vagy **Havonta** lehetőséget, majd válassza ki a napot és az időpontot:
   a. Kattintson vagy koppintson az óra, perc vagy DE/DU mezőre.
   b. Görgesse, amíg a kívánt érték meg nem jelenik a többi mezővel azonos szinten.
   c. Kattintson vagy koppintson az időbeállító mezők körüli fehér részre.
   d. Mindegyik mező esetében ismételje meg, amíg a helyes ütemezést ki nem választotta.
3. A következő négy típusú elem van felsorolva:
   - **Lomtár**—Az összes Lomtárban található tételt megsemmisíti.
   - **Ideiglenes rendszerfájlok**—Megsemmisíti az összes fájlt, amely a rendszer ideiglenes mappájában található. Az alábbi környezeti változókat a következő sorrendben keresik, és az elsőnek megtalált útvonal tekintendő rendszermappának:
     - TMP
     - TEMP
   - **Ideiglenes internetes fájlok**—Megsemmisíti a weboldalak, képek és médiafájlok másolatait, melyeket a webböngésző mentett el a gyorsabb megtekintés érdekében.
   - **Cookies**—Megsemmisíti a weboldalak által, a számítógépen, – a preferenciák (például bejelentkezési adatok) mentése érdekében – elmentett összes fájlt.

   Ha kijelölte, akkor ezek az elemek az ütemezett időpontban megsemmisítésre kerülnek.
4. További, megsemmisítendő elemek kiválasztásához:
   a. Az **Ütemezett megsemmisítési lista** pont alkatt kattintson vagy koppintson a **Mappa hozzáadása** lehetőségre, majd navigáljon a fájlhoz vagy mappához.
   b. Kattintson vagy koppintson a **Megnyitás** pontra, majd kattintson vagy koppintson az **OK**-ra.

Elem eltávolításához az Ütemezett megsemmisítési listából törölje az elemhez tartozó jelölőnégyzet kijelölését.

A szabad lemezterület teljes törlése ütemezésének beállítása

A szabad lemezterület teljes törlése nem biztosít további biztonságot a megsemmisített elemeknek.

1. Nyissa meg a File Sanitizer-t, majd kattintson vagy koppintson a **Beállítások** pontra.
2. Későbbi időpont ütemezéséhez a kiválasztott elemek szabad lemezterület teljes törlésére, a **Szabad lemezterület teljes törlésének ütemezése** pont alatt válassza a **Soha**, **Egyszer**, **Naponta**, **Hetente** vagy **Havonta** lehetőséget, majd válassza ki a napot és az időpontot:
   a. Kattintson vagy koppintson az óra, perc vagy DE/DU mezőre.
   b. Görgesse, amíg a kívánt időpont meg nem jelenik a többi mezővel azonos szinten.
   c. Kattintson vagy koppintson az időbeállító mezők körüli fehér részre.
   d. Ismételje meg, amíg a helyes ütemezést ki nem választotta.

MEGJEGYZÉS: A szabad lemezterület teljes törlése művelet jelentős ideig eltarthat. Győződjön meg róla, hogy számítógépe csatlakozik a váltakozó áramú hálózathoz. Habár a szabad lemezterület teljes törlése a háttérben történik, a számítógép teljesítményét befolyásolhatja a processzor megnövekedett használata. A szabad lemezterület teljes törlése órák után is elvégezhető, vagy amikor a számítógép nincs használatban.

Fájlok védelme a megsemmisítéstől

Fájlok és mappák védelméhez a megsemmisítéstől:

1. Nyissa meg a File Sanitizer-t, majd kattintson vagy koppintson a **Beállítások** pontra.
2. Az **Sosem megsemmisítendő lista** pont alatt kattintson vagy koppintson a **Mappa hozzáadása** lehetőségre, majd navigáljon a fájlhoz vagy mappához.
3. Kattintson vagy koppintson a **Megnyitás** pontra, majd kattintson vagy koppintson az **OK**-ra.

MEGJEGYZÉS: A listában található fájlok védettek, amíg a listában maradnak.

Elem eltávolításához a kizárások listából törölje az elemhez tartozó jelölőnégyzet kijelölését.

Általános feladatok

Az alábbi feladatok elvégzésére használja a File Sanitizer-t:

- **A File Sanitizer ikon használata a mnegsemmisítés kezdeményezéséhez**—Húzza a fájlokat a **File Sanitizer** ikonra a Windows asztalon. A részletekért keresse fel a következő oldalt: A File Sanitizer ikon használata, 42. oldal.
- **Adott elem vagy az összes kiválasztott elem manuális megsemmisítése**—Tételek megsemmisítése bármikor, anélkül, hogy ütemezett megsemmisítési időpontra kellene várni. A részletekért keresse fel a következő oldalakat: Jobb egérgombos kattintásos megsemmisítés, 42. oldal vagy Megsemmisítési művelet manuális kezdése, 42. oldal.

- **A szabad lemezterület teljes törlésének manuális aktiválása**—Bármikor aktiválja a szabad lemezterület teljes törlését. A részletekért keresse fel a következő oldalt: A szabad lemezterület teljes törlésének manuális kezdése, 43. oldal.
- **Naplófájlok megtekintése**—A megsemmisítési és a szabad lemezterület teljes törlése naplófájlok megtekintése, melyek hibákat tartalmaznak vagy nem sikerültek az utolsó megsemmisítési vagy szabad lemezterület teljes törlése művelete során. A részletekért keresse fel a következő oldalt: A naplófájlok megtekintése, 43. oldal.

MEGJEGYZÉS: A megsemmisítés vagy szabad lemezterület teljes törlése művelet jelentős ideig eltarthat. Habár a megsemmisítés és a szabad lemezterület teljes törlése a háttérben történik, a számítógép teljesítményét befolyásolhatja a processzor megnövekedett használata.

A File Sanitizer ikon használata

VIGYÁZAT! A megsemmisített elemeket nem lehet visszaállítani. Alaposan fontolja meg, milyen elemeket választ ki a manuális megsemmisítésre.

Amikor manuálisan kezd megsemmisítési műveletet, a File Sanitizer nézet szokásos megsemmisítési listája megsemmisítésre kerül (lásd: Telepítési eljárások, 39. oldal).

A következő módok egyikével kezdhet manuálisan megsemmisítési műveletet:

1. Nyissa meg a File Sanitizer programot (lásd: A File Sanitizer megnyitása, 39. oldal), majd kattintson vagy koppantson a **Megsemmisítés** lehetőségre.
2. Amikor megnyílik egy megerősítő párbeszédablak, akkor győződjön meg arról, hogy be vannak jelölve a megsemmisíteni kívánt elemek, majd kattintson vagy koppintson az **OK**-ra.

– vagy –

1. Jobb egérgombbal kattintson vagy koppintson a **File Sanitizer** ikonra a Windows asztalon, és tartsa úgy, majd kattintson vagy koppintson a **Megsemmisítés most** elemre.
2. Amikor megnyílik egy megerősítő párbeszédablak, akkor győződjön meg arról, hogy be vannak jelölve a megsemmisíteni kívánt elemek, majd kattintson vagy koppintson a **Megsemmisítés** pontra.

Jobb egérgombos kattintásos megsemmisítés

VIGYÁZAT! A megsemmisített elemeket nem lehet visszaállítani. Alaposan fontolja meg, milyen elemeket választ ki a manuális megsemmisítésre.

Ha a **Jobb egérgombos megsemmisítés engedélyezése** elemet kiválasztotta a File Sanitizer nézetben, akkor a következőképp semmisíthet meg egy elemet:

1. Navigáljon a megsemmisíteni kívánt dokumentumhoz vagy mappához.
2. Jobb egérgombbal kattintson vagy koppintson a fájlra vagy mappára, és tartsa úgy, majd válassza ki a **HP File Sanitizer – Megsemmisítés** elemet.

Megsemmisítési művelet manuális kezdése

VIGYÁZAT! A megsemmisített elemeket nem lehet visszaállítani. Alaposan fontolja meg, milyen elemeket választ ki a manuális megsemmisítésre.

Amikor manuálisan kezd megsemmisítési műveletet, a File Sanitizer nézet szokásos megsemmisítési listája megsemmisítésre kerül (lásd: Telepítési eljárások, 39. oldal).

A következő módok egyikével kezdhet manuálisan megsemmisítési műveletet:

1. Nyissa meg a File Sanitizer programot (lásd: A File Sanitizer megnyitása, 39. oldal), majd kattintson vagy koppantson a **Megsemmisítés** lehetőségre.
2. Amikor megnyílik egy megerősítő párbeszédablak, akkor győződjön meg arról, hogy be vannak jelölve a megsemmisíteni kívánt elemek, majd kattintson vagy koppintson az **OK**-ra.

– vagy –

1. Jobb egérgombbal kattintson vagy koppintson a **File Sanitizer** ikonra a Windows asztalon, és tartsa úgy, majd kattintson vagy koppintson a **Megsemmisítés most** elemre.
2. Amikor megnyílik egy megerősítő párbeszédablak, akkor győződjön meg arról, hogy be vannak jelölve a megsemmisíteni kívánt elemek, majd kattintson vagy koppintson a **Megsemmisítés** pontra.

A szabad lemezterület teljes törlésének manuális kezdése

Amikor manuálisan kezd teljes törlési műveletet, a File Sanitizer nézet szokásos megsemmisítési listája teljes törlésre kerül (lásd: Telepítési eljárások, 39. oldal).

A következő módok egyikével kezdhet manuálisan teljes törlési műveletet:

1. Nyissa meg a File Sanitizer programot (lásd: A File Sanitizer megnyitása, 39. oldal), majd kattintson vagy koppantson a **Teljes törlés** lehetőségre.
2. Amikor megnyílik a megerősítő párbeszédablak, akkor kattintson vagy koppintson az **OK**-ra.

– vagy –

1. Jobb egérgombbal kattintson vagy koppintson a **File Sanitizer** ikonra a Windows asztalon, és tartsa úgy, majd kattintson vagy koppintson a **Teljes törlés most** elemre.
2. Amikor megnyílik a megerősítő párbeszédablak, akkor kattintson vagy koppintson a **Teljes törlés** pontra.

A naplófájlok megtekintése

Minden alkalommal, amikor megsemmisítési vagy szabad lemezterület teljes törlési műveletet hajt végre, naplófájl készül a hibákról vagy sikertelenségekről. A naplófájlok mindig frissítésre kerülnek a legutóbbi megsemmisítési vagy szabad lemezterület teljes törlési művelet szerint.

MEGJEGYZÉS: A sikeresen megsemmisített vagy teljesen törölt fájlok nem jelennek meg a naplófájlokban.

Egy naplófájl készül a megsemmisítési műveletekhez, és egy másik naplófájl a szabad lemezterület teljes törlése műveletekhez. Mindkét naplófájl a merevlemezen, az alábbi mappákban található:

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

64 bites rendszerek esetén a naplófájlok a merevlemezen, az alábbi mappákban találhatók:

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

7 HP Device Access Manager (csak bizonyos modelleknél)

A HP eszközhozzáférés-kezelő szabályozza a hozzáférést az adatokhoz úgy, hogy letiltja az adatátviteli eszközöket.

MEGJEGYZÉS: Néhány külső kezelőeszközt (HID)/beviteli eszközt (például egér, billentyűzet, TouchPad és ujjlenyomatolvasó) nem szabályoz a Device Access Manager. További információ itt olvasható: Kezeletlen eszközosztályok, 47. oldal.

A Windows® operációs rendszer rendszergazdái a HP eszközhozzáférés-kezelőt használják a rendszeren található eszközökhöz való hozzáférés szabályozására és az illetéktelen hozzáférés elleni védelemre:

- Az eszközprofilokat az egyes felhasználóknak hozzák létre, hogy meghatározzák azokat az eszközöket, amelyekhez a hozzáférés engedélyezett vagy tiltott.
- A Pont időben hitelesítés (JITA) lehetővé teszi, hogy előre meghatározott felhasználók hitelesítsék magukat, hogy egyébként megtagadott eszközökhöz hozzáférjenek.
- A rendszergazdák és megbízható felhasználók kizárhatók a korlátozás alól a Device Access Manager által kijelölt eszközhozzáférésre vonatkozóan, ha hozzáadja őket az Eszköz rendszergazdai csoportjához. E csoport tagságát a Haladó beállításokban kezelheti.
- Az eszközökhöz való hozzáférés garantálható vagy megtagadható a csoporttagság alapján vagy egyedi felhasználók esetén.
- Olyan eszközosztályok esetén, mint a CD-ROM meghajtók és DVD meghajtók, az olvasási és írási hozzáférés külön engedélyezhető vagy megtagadható.

A HP eszközhozzáférés-kezelő automatikusan az alábbi beállításokkal konfigurált a HP Client Security telepítő varázsló elvégzése során:

- A Pont időben hitelesítés (JITA) cserélhető adathordozó engedélyezett a rendszergazdáknak és felhasználóknak.
- Az eszköz szabálya engedélyezi a teljes hozzáférést más eszközökhöz.

Az eszközhozzáférés-kezelő megnyitása

1. A kezdőképernyőn kattintson vagy koppintson a **HP Client Security** alkalmazásra (Windows 8).

   – vagy –

   A Windows asztalon kétszer kattintson vagy duplán koppintson a **HP Client Security** ikonra az értesítési területen, mely a feladatsor jobb oldalán található.

2. Az **Eszköz** alatt kattintson vagy koppintson az **Eszköz engedélyei** elemre.

   - A szokásos felhasználók megtekinthetik az aktuális eszközhozzáférésüket (lásd: Felhasználói nézet, 45. oldal).
   - A rendszergazdák megtekinthetik és módosíthatják a számítógépen jelenleg konfigurált eszközhozzáférést, ha rákattintsanak vagy koppintanak a **Módosítás** elemre, majd megadják a rendszergazdai jelszavukat (lásd: Rendszernézet, 45. oldal).

Felhasználói nézet

Amikor az **Eszköz engedélyezése** lehetőséget választja, akkor megjelenik a Felhasználói nézet. A szabálytól függően a szokásos felhasználók és rendszergazdák megtekinthetik a saját hozzáféréseiket a készülékosztályokhoz vagy egyedi készülékekhez ezen a számítógépen.

- **Aktuális felhasználó**—A jelenleg bejelentkezett felhasználó neve jelenik meg.
- **Eszközosztály**—Megjelennek az eszköztípusok.
- **Hozzáférés**—Megjelenik az eszköztípusokhoz vagy adott eszközökhöz jelenleg konfigurált hozzáférés.
- **Időtartam**—Megjelenik a CD/DVD-ROM meghajtókhoz vagy cserélhető lemezes meghajtókhoz való hozzáférésének az időkorlátja.
- **Beállítások**—A rendszergazdák megváltoztathatják, hogy mely meghajtók rendelkezzenek az eszközhozzáférés-kezelő által szabályozott hozzáféréssel.

Rendszernézet

A rendszernézetben a rendszergazdák engedélyezhetik vagy megtagadhatják a számítógép eszközeihez a hozzáférést a felhasználók vagy a rendszergazdák csoportjának.

▲ A rendszergazdák hozzáférhetnek a rendszernézethez, ha rákattintanak vagy koppintanak a **Módosítás** elemre, és megadják a rendszergazdai jelszót, majd választanak az alábbi pontok közül:

- **Eszközhozzáférés-kezelő**—A HP eszközhozzáférés-kezelő be- vagy kikapcsolásához a Pont időben hitelesítéssel kattintson vagy koppintson a **Be** vagy **Ki** gombra.
- **Felhasználók és csoportok ezen a számítógépen**—Megjeleníti a felhasználók vagy rendszergazdák csoportját, akik hozzáférése engedélyezett vagy elutasított a kiválasztott eszközosztályokhoz.
- **Eszközosztály**—Megjeleníti azon eszközosztályokat és eszközöket, melyek telepítve vannak a rendszeren, vagy melyeket lehet, hogy a rendszer korábban telepített. A lista bővítéséhez kattintson **+** ikonra. Látható az összes, számítógéphez csatlakoztatott eszköz, és kibővült a rendszergazdák és felhasználók csoportja a tagságuk mutatása érdekében. Az eszközlista frissítéséhez kattintson a kerek nyíl (frissítés) ikonra.
  - Az eszközosztályokra általában védelem vonatkozik. Ha a hozzáférés **Engedélyezett**, a kiválasztott felhasználó vagy csoport hozzáféréssel rendelkezik majd az eszközosztályban minden eszközhöz.
  - Védelem is vonatkozhat az adott eszközhöz.
  - Ha konfigurálja a Pont időben hitelesítést (JITA), azzal lehetővé teszi a felhasználói hozzáférés kiválasztását a DVD-/CD-ROM-meghajtókhoz vagy a cserélhető lemezes meghajtókhoz, azok hitelesítésével. További információ itt olvasható: JITA konfigurálás, 46. oldal.
  - Engedélyezze vagy tagadja meg más eszközosztályokhoz a hozzáférést, például cserélhető adathordozók (USB flash meghajtók), soros és párhuzamos portok, Bluetooth® eszközök, modemes eszközök, PCMCIA/ExpressCard eszközök, 1394 eszközök, ujjlenyomat-olvasó és intelligenskártya-olvasó. Ha nem engedélyezett az ujjlenyomat-olvasó és az intelligenskártya-olvasó, akkor használhatók hitelesítő adatokként, de nem használhatók a munkamenet szabályszintjén.

MEGJEGYZÉS: Ha a Bluetooth-eszközöket hitelesítő adatokként használják, akkor nem korlátozható a Bluetooth-eszköz hozzáférése az Eszközhozzáférés-kezelő szabályában.

- Amikor kiválaszt egy beállítást a csoportnál vagy az eszközosztály szintjén, és megkérdezik, hogy kívánja-e a beállítást a gyermek tárgyakra is alkalmazni:

  Igen—A beállítás automatikusan kitöltésre kerül.

  Nem—A beállítás nem kerül automatikusan kitöltésre.

- Az olvasási és írási műveletek hozzáférésének külön engedélyezésével vagy megtagadásával tovább szabályozható néhány eszközosztály, például a DVD és CD-ROM.

MEGJEGYZÉS: A rendszergazdák csoportja nem adható hozzá a Felhasználói listához.

- **Hozzáférés**—Kattintson vagy koppintson a lefelé nyílra, majd válasszon egyet az alábbi hozzáféréstípusok közül, hogy engedélyezze vagy megtagadja a hozzáférést:
  - **Engedélyez – Teljes hozzáférés**
  - **Engedélyez – Csak olvasás**
  - **Engedélyez – JITA szükséges**—További információ: JITA konfigurálás, 46. oldal.

    Ha ezt a hozzáféréstípust választja ki az **Időtartam** alatt, akkor kattintson vagy koppintson a lefelé nyílra egy időkorlát kiválasztásához.
  - **Visszautasítás**
- **Időtartam**—Kattintson vagy koppintson a lefelé nyílra, hogy kiválasszon egy időkorlátot a CD/DVD-ROM meghajtókhoz vagy cserélhető lemezes meghajtókhoz való hozzáféréshez (lásd: JITA konfigurálás, 46. oldal).

JITA konfigurálás

A JITA konfigurálás lehetővé teszi, hogy a rendszergazda megtekintse és módosítsa a felhasználók és csoportok listáját, melyeket az eszközök hozzáféréséhez engedélyeztek a Pont időben hitelesítés (JITA) segítségével.

A JITA lehetővé teszi, hogy a felhasználók hozzáférjenek néhány eszközhöz, melyekhez az **Eszközhozzáférés-kezelő** nézetben létrehozott szabályokat korlátozták.

A JITA időszak beállított számú perchez vagy korlátlanul engedélyezhető. Korlátlan felhasználónak lesz hozzáférése az eszközhöz onnantól kezdve, hogy hitelesítik, addig, amíg ki nem jelentkezik a rendszerből.

Ha a felhasználó korlátozott JITA időszakot kap, akkor a JITA időszak lejárta előtt egy perccel megkérdezik a felhasznbálót, hogy szeretné-e meghosszabbítani a hozzáférést. Amikor a felhasználó kijelentkezik a rendszerből vagy egy másik felhasználó bejelentkezik, a JITA időszak lejár. Legközelebb, amikor a felhasználó bejelentkezik és megpróbál hozzáférni egy JITA-engedélyezett eszközhöz, megkéri a rendszer, hogy adja meg a hitelesítő adatokat.

A JITA az alábbi eszközosztályoknál érhető el:

- DVD/CD-ROM meghajtók
- Cserélhető lemezmeghajtók

JITA házirend létrehozása egy felhasználóhoz vagy csoporthoz

A rendszergazdák engedélyezhetik a felhasználóknak vagy csoportoknak a hozzáférést az eszközökhöz a Pont időben hitelesítés (JITA) segítségével.

1. Indítsa el az **Eszközhozzáférés-kezelőt**, majd kattintson vagy koppintson a **Módosítás** gombra.
2. Válassza ki a felhasználót vagy csoportot, majd a **Cserélhető lemezmeghajtók** vagy a **DVD-/CD-ROM-meghajtók Hozzáférés** pontja alatt kattintson vagy koppintson a lefelé nyílra, majd válassza az **Engedélyez – JITA szükséges** elemet.
3. Az **Időtartam** alatt kattintson vagy koppintson a lefelé nyílra, hogy kiválassza a JITA hozzáférés időtartamát.

A felhasználónak ki kell jelentkeznie, majd ismét be kell jelentkeznie az új JITA beállítás alkalmazásához.

JITA házirend letiltása egy felhasználóhoz vagy csoporthoz

A rendszergazdák letilthatják a felhasználóknak vagy csoportoknak a hozzáférést az eszközökhöz a Pont időben hitelesítés segítségével.

1. Indítsa el az **Eszközhozzáférés-kezelőt**, majd kattintson vagy koppintson a **Módosítás** gombra.
2. Válassza ki a felhasználót vagy csoportot, majd a **Cserélhető lemezmeghajtók** vagy a **DVD-/CD-ROM-meghajtók Hozzáférés** pontja alatt kattintson vagy koppintson a lefelé nyílra, majd válassza az **Megtagad** elemet.

Amikor a felhasználó bejelentkezik és megpróbál hozzáférni az eszközhöz, a hozzáférés nem lesz engedélyezett.

Beállítások

A **Beállítások** nézet lehetővé teszi, hogy a rendszergazdák megtekintsék és módosítsák a meghajtókat, amelyekhez az Eszközhozzáférés-kezelő által szabályozott hozzáférése van.

MEGJEGYZÉS: Az eszközhozzáférés-kezelőt engedélyezni kell, amikor a meghajtók betűjelének listája konfigurált (lásd: Rendszernézet, 45. oldal).

Kezeletlen eszközosztályok

A HP eszközhozzáférés-kezelő nem kezeli az alábbi eszközosztályokat:

- Bemeneti/kimeneti eszközök
  - CD-ROM
  - Lemezmeghajtó
  - Floppy lemez vezérlő (FDC)
  - Merevlemez vezérlő (HDC)
  - Külső kezelőeszköz (HID) osztálya
  - Infravörös külső kezelőeszközök
  - Egér
  - Többportos soros
  - Billentyűzet

- Plug and play (PnP) nyomtatók
- Nyomtató
- Nyomtatófrissítés

- Tápkapcsoló
  - Fejlett energiagazdálkodási (APM) támogatás
  - Akkumulátor
- Egyebek
  - Számítógép
  - Dekóder
  - Kijelző
  - Intel® egyesített kijelzőmeghajtó
  - Legacard
  - Adathordozó-meghajtó
  - Adathordozó-töltő
  - Memóriatechnológia
  - Monitor
  - Multifunkció
  - Net kliens
  - Net szolgáltatás
  - Net átvitel
  - Processzor
  - SCSI adapter
  - Biztonsági gyorsító
  - Biztonsági eszközök
  - Rendszer
  - Ismeretlen
  - Hangerő
  - Hangerő pillanatkép

8 HP Trust Circles

A HP Trust Circles olyan fájl és dokumentum biztonsági alkalmazás, mely a mappafájlok titkosítását kombinálja megfelelő megbízható dokumentummegosztási képességgel. Az alkalmazás titkosítja a felhasználóra jellemző mappákban található fájlokat, és megbízható körökön belül védi azokat. Amint védettek, a fájlokat csak a bizalmi kör tagjai használhatják és oszthatják meg. Ha egy védett fájlt nem tag kap meg, a fájl titkosított marad és a nem tag nem érheti el a tartalmát.

A Trust Circles megnyitása

1. A kezdőképernyőn kattintson vagy koppintson a **HP Client Security** alkalmazásra.

   – vagy –

   A Windows asztalon kétszer kattintson a **HP Client Security** ikonra az értesítési területen, mely a feladatsor jobb oldalán található.

2. Az **Adatok** alatt kattintson vagy koppintson a **Trust Circles** elemre.

Első lépések

Kétféle módon küldhet e-mailes meghívásokat és válaszolhat azokra:

- **A Microsoft® Outlook segítségével**—A Trust Circles és a Microsoft Outlook használata minden Trust Circle imeghívás feldolgozását automatikusan végzi, illetve más Trust Circle felhasználóknak válaszol.
- **Gmail, Yahoo, Outlook.com vagy más e-mail szolgáltatásaok (SMTP) használata**—Neve, e-mail címe és jelszava megadásakor a Trust Circles az Ön e-mail szolgáltatását használva küld e-mailes meghívásokat a bizalmi köréhez csatalkozásra kiválasztott tagoknak.

Az alap profil beállításához:

1. Adja meg a nevét és e-mail címét, majd kattintson vagy koppintson a **Tovább** gombra.

   A nevet minden tag láthatja, akit meghív a körhöz csatlakozásra. Az e-mail cím a meghívások elküldésére, fogadására és válaszolására használatos.

2. Adja meg az e-mail címhez tartozó jelszót, majd kattintson vagy koppintson a **Tovább** gombra.

   Küld a rendszer egy tesz e-mailt, hogy ellenőrizze, hogy pontosak-e az e-mail beállítások.

   MEGJEGYZÉS: A számítógépnek csatlakoznia kell hálózathoz.

3. A **Trust Circle név** mezőben adja meg a Trust Circle nevét, majd kattintson vagy koppintson a **Tovább** gombra.

4. Adjon hozzá tagokat és mappákat, majd kattintson vagy koppintson a **Tovább** pontra. A Trust Circle bármilyen, kiválasztott mappával létrehozásra kerül, és e-mailes meghívásokat küld bármilyen, kiválasztott tagoknak. Ha bármilyen okból kifolyóan egy meghívás nem küldhető el, akkor értesítés jelenik meg. A tagok ismét meghívhatók, bármikor a Trust Circle nézetből, ha a **Saját Trust Circles** pontra kattint, majd kétszer kattint vagy duplán koppint a Trust Cirle-re. További információ itt olvasható: Trust Circles, 50. oldal.

Trust Circles

Létrehozhat egy bizalmi kört az első telepítés közben, miután megadta az e-mail címét, vagy a Trust Circle nézetben:

▲ A Trust Circle nézetben kattintson vagy koppintson a **Trust Circle létrehozása** pontra, majd adja meg a Trust Circle nevét.

- Tagok hozzáadásához Trust Circle-höz, kattintson vagy koppintson az **M+** ikonra a **Tagok** alatt, majd kövesse a képernyőn megjelenő utasításokat.
- Mappák hozzáadásához Trust Circle-höz, kattintson vagy koppintson a **+** ikonra a **Mappák** alatt, majd kövesse a képernyőn megjelenő utasításokat.

Mappák hozzáadása Trust Circle-höz

Mappák hozzáadása új Trust Circle-höz:

- Trust Circle létrehozása közben mappákat adhat hozzá a **Mappák** mellett a **+** ikonra kattintva vagy koppintva, majd a képernyőn megjelenő utasításokat követve.

  – vagy –

- A Windows Explorer-ben jobb egérgombbal kattintva vagy koppintva és nyomva tartva egy mappát, mely jelenleg a Trust Circle része, válassza a **Trust Circle** pontot, majd a **Trust Circle létrehozása mappából** elemet.

TIPP: Kiválaszthat egy vagy több mappát.

Mappák hozzáadása meglévő Trust Circle-höz:

- A Trust Circle nézetben kattintson a **Saját Trust Circles** pontra, kétszer kattintson vagy duplán koppintson a meglévő Trust Circle-re, hogy megjelenjenek az aktuális mappák, kattintson vagy koppintson a **+** ikonra a **Mappák** mellett, majd kövesse a képernyőn megjelenő utasításokat.

  – vagy –

- A Windows Explorer-ben jobb egérgombbal kattintva vagy koppintva és nyomva tartva egy mappát, mely jelenleg a Trust Circle része, válassza a **Trust Circle** pontot, majd a **Meglévő Trust Circle hozzáadása mappából** elemet.

TIPP: Kiválaszthat egy vagy több mappát.

Amint mappát adott egy Trust Circle-höz, a Trust Circles automatikusan titkosítja a mappát és a tartalmát. Amint az összes fájl titkosított, értesítés jelenik meg. Továbbá megjelenik egy zöld zárolás szimbólum az összes titkosított mappa ikonján és a mappában találhatók fájlok ikonjain. Ez jelzi, hogy teljesen védettek.

Tagok hozzáadása Trust Circle-höz

Három lépés szükséges tagok hozzáadásához Trust Circle-höz:

1. **Meghívás**—Először a Trust Circle tulajdonosa meghívja a tago(ka)t. A meghívó e-mail több felhasználónak vagy listáknak/csoportoknak elküldhető.
2. **Elfogadás**—A meghívott megkapja a meghívást, és eldönti, hogy elfogadja vagy elutasítja. Ha a meghívott elfogadja a meghívást, e-mailes választ küld a meghívónak. Ha a meghívást csoportnak küldték, akkor mindegyik tag kap meghívást és dönthet az elfogadásról vagy elutasításról.
3. **Regisztrálás**—A meghívónak van egy utolsó lehetőségle, hogy eldöntse hozzáadja-e a tagot a Trust Circle-höz. A meghívó eldönti, hogy regisztrálja-e a tagot. E-mailt küld a meghívottnak a válasza megerősítésére. A meghívó és a meghívott opcionálisan megerősítheti a Meghívási folyamat biztonságát. A meghívottnak megjelenik egy megerősítő kód, melyet be kell olvasnia a meghívónak telefonon. Amint megerősítésre került a kód, a meghívó kiküldheti az utolsó regisztrá e-mailt.

Tagok hozzáadása új Trust Circle-höz:

▲ Trust Circle létrehozása közben tagokat adhat hozzá a **Tagok** alatt az **M+** ikonra kattintvag vagy koppintva, majd a képernyőn megjelenő utasításokat követve.

- Ha Outlook-ot használ, válassza ki a névjegyeket a címjegyzékből, majd kattintson az **OK**-ra.
- Ha más e-mail szolgáltatást használ, akkor vagy adja az új címeket kézzel a Trust Circle-höz, vagy visszanyerheti azokat a Trust Circle-ben regisztrált e-mail címekből.

Tagok hozzáadása meglévő Trust Circle-höz:

▲ A Trust Circle nézetben kattintson a **Saját Trust Circles** pontra, kétszer kattintson vagy duplán koppintson a meglévő Trust Circle-re, hogy megjelenjenek az aktuális tagok, kattintson vagy koppintson az **M+** ikonra a **Tagok** alatt, majd kövesse a képernyőn megjelenő utasításokat.

- Ha Outlook-ot használ, válassza ki a névjegyeket a címjegyzékből, majd kattintson az **OK**-ra.
- Ha más e-mail szolgáltatást használ, akkor vagy adja az új címeket kézzel a Trust Circle-höz, vagy visszanyerheti azokat a Trust Circle-ben regisztrált e-mail címekből.

Fájlok hozzáadása Trust Circle-höz

Az alábbi módok egyikével adhat hozzá fájlokat Trust Circle-höz:

- Másolja vagy mozgassa a fájlt meglévő Trust Circle mappába.

  – vagy –

- A Windows Explorer-ben jobb egérgombbal kattintva vagy koppintva és nyomva tartva egy fájlt, mely jelenleg nem titkosított, válassza a **Trust Circle** pontot, majd a **Titkosítás** elemet. Megkérik majd, hogy válassza ki a Trust Circle-t, amelyhez a fájlt hozzá kell adni.

TIPP: Kiválaszthat egy vagy több fájlt.

Titkosított mappák

Egy Trust Circle minden tagja megtekintheti és szerkesztheti a fájlokat, melyek ahhoz a Trust Circle-höz tartoznak.

MEGJEGYZÉS: A Trust Circle Manager/Reader nem szinkronizálja a fájlokat a tagok között.

A fájlokat a létező módokkal kell megosztani, azaz e-mail, ftp vagy felhő tárolási szolgáltató segítségével. Trust Circle-be másolt, vitt vagy ott létrehozott fájlok azonnal védettek.

Mappák eltávolítása Trust Circle-ből

A mappa eltávolítása Trust Circle-ből visszafejti a mappát és összes tartalmát és eltávolítja a védelmét.

- A Trust Circle nézetben kattintson vagy koppintson a **Saját Trust Circles** pontra, kétszer kattintson vagy duplán koppintson a meglévő Trust Circle-re, hogy megjelenjenek az aktuális mappák, majd kattintson vagy koppintson az **Iomtár** ikonra a mappák alatt.

  – vagy –

- A Windows Explorer-ben jobb egérgombbal kattintva vagy koppintva és nyomva tartva egy mappát, mely jelenleg a Trust Circle része, válassza a **Trust Circle** pontot, majd az **Eltávolítás Trust Circle-ből** elemet.

TIPP: Kiválaszthat egy vagy több mappát.

Fájl eltávolítása Trust Circle-ből

Fájl eltávolításához Trust Circle-ből a Windows Explorer-ben jobb egérgombbal kattintson vagy koppintson és tartsa lenyomva a fájlt, mely jelenleg nem titkosított, válassza a **Trust Circle** pontot, majd a **Fájl visszafejtése** elemet.

Tagok eltávolítása Trust Circle-ből

Olyan tag, aki nem teljesen regisztrált, nem távolítható el a Trust Circle-ből. Alternatíva lenne új Trust Circle létrehozása az összes többi taggal, az összes fájl és mappa átvitele az új Trust Circle-be, majd a régi Trust Circle törlése. Ez biztosítja, hogy ne legyen hozzáférhető minden új fájl, melyet a tagok kapnak, de minden, amit korábban megosztottak hozzáférhető marad a régi Trust Circle tagjainak.

Ha a tag nem teljesen regisztrált (vagy meghívták a tagok a Trust Circle-be vagy nem fogadta el a meghívást a Trust Circle-be), az alábbi módok egyikével távolíthatja el a tagot a Trust Circle-ből:

- A Trust Circle nézetben kattintson vagy koppintson a **Saját Trust Circles** elemre, majd kétszer kattintson vagy duplán koppintson a Trust Circle-re, hogy megmutassa a tagok aktuális listáját. Kattintson vagy koppintson a **Iomtár** ikonra az eltávolítandó tag neve alatt.
- A Trust Circle nézetben kattintson vagy koppintson a **Tagok** pontra, majd kétszer kattintson vagy duplán koppintson a tagra, hogy megmutassa azon Trust Circle-t, melyben tag. Kattintson vagy koppintson a **Iomtár** ikonra a Trust Circle mellett, hogy abból a Trust Circle-ből eltávolítsa a tagot.

Trust Circle törlése

Trust Circle törléséhez tulajdon szükséges.

- A Trust Circle nézetben kattintson vagy koppintson a **Saját Trust Circles** pontra, majd a **Iomtár** ikonra a törlendő Trust Circle mellett.

  Ez eltávolítja a Trust Circle-t az oldalról és e-mailt küld az összes tagnak, melyben tájékoztat a Trust Circle törléséről. Minden fájl vagy mappa, melyet ez a Trust Circle tartalmaz visszafejtett.

Beállítások

A Trust Circle nézetben kattintson vagy koppintson a **Beállítások** pontra. Három lap jelenik meg

- **E-mail beállításai**

Lehetőség	Leírás
Felhasználónév	Megjelenik a jelenleg használt felhasználónév. A módosításhoz adjon meg új felhasználónevet a szövegdobozban. A módosítások automatikusan mentésre kerülnek.
E-mail cím	Megjelenik a jelenleg használt e-mail cím. A módosításhoz kattintson vagy koppintson az **E-mail beállítások módosítása** pontra, majd kövesse a képernyőn megjelenő utasításokat.
Új tag megerősítése	Válasszon a következő lehetőségek közül: ◦ **Megerősítés automatikusan**—Miután megkapta a meghívottól az elfogadást, megerősítésre kerül a Trust Circle-ben manuális bevitel nélkül, és megerősítő e-mailt küld a rendszer a meghívottnak. ◦ **Megerősítés kézzel**—Miután megkapta a meghívottól az elfogadást, kézi bevitel szükséges az új tagok regisztrálásához a Trust Circle-be, majd megerősítő e-mailt küld a rendszer a meghívottnak. ◦ **Igazolás szükséges**—Miután megkapta a meghívottól az elfogadást, igazoló kód szükséges a meghívott teljes regisztrálásához. A Trust Circle tulajdonosának fel kell vennie a kapcsolatot a meghívottal, és meg kell kapnia tőle az igazoló kódot. A helyes kód megadása után kiküldésre kerül a megerősítő e-mail.
Időszakos hitelesítés	Időszakos hitelesítés szükséges, hogy a felhasználó megadja a Windows-jelszót az adott időtúllépés után (percben rögzítve), és az érzékeny művelet közben is. Ez a beállítás lehetővé teszi, hogy a felhasználók be- vagy kikapcsolják a hitelesítést.
Hitelesítés időtúllépése	Válassza ki a meghatározott időtúllépési időszakot (percben rögzítve) a hitelesítés szükségessége előtt.
Ne mutassa a megerősítő üzenetet.	Jelölje ki a jelölőnégyzetet a megerősítő üzenetek megmutatásának letiltásához, vagy törölje a jelölőnégyzetet, hogy megjelenjenek a megerősítő üzenetek.
Szeretnék segíteni javítani a HP Trust Circles programot névtelen felhasználáskövetéssel	Jelölje ki a jelölőnégyzetet, hogy részt vegyen a programban, vagy törölje a jelölőnégyzetet, ha nem szeretne részt venni.

- **Biztonsági mentés/visszaállítás**

Lehetőség	Leírás
Biztonsági mentés	Átmásolja a Trust Circle Manager/Reader alkalmazás adatait (beállítások és Trust Circles) egy biztonságimásolat-fájlba. Összeomlás vagy rendszerhiba esetén ezt a fájlt használhatja a Trust Circles új telepítésének visszaállításához a fájlban mentett állapotban. **MEGJEGYZÉS:** Csak a Trust Circle alkalmazás adatai kerülnek mentésre (Trust Circles, beállítások és tagok). A Trust Circle mappa tényleges fájljai nem kerülnek biztonsági mentésre. Azokat a fájlokat külön kell menteni. A Trust Circle beállítások és felhasználói adatok biztonsági mentéséhez: **1.** Kattintson vagy koppintson a **Biztonsági mentés** gombra. **2.** Válasszon fájlnevet és mappát a biztonságimásolat-fájlnak, majd kattintson vagy koppintson a **Mentés** gombra. **3.** Adjon meg jelszót, erősítse meg, majd kattintson vagy koppintson az **OK**-ra. Ez a jelszó kell majd a fájl visszaállításához.
Visszaállítás	Visszaállítja a beálíltásokat és Trust Circles-ket egy biztonságimásolat-fájlból általában rendszerösszeomlás után vagy ha másik számítógépre viszi át. A Trust Circles Manager beállításainak és a felhasználói adatok visszaállításához: **1.** Kattintson vagy koppintson az **Visszaállítás** gombra. **2.** Menjen a biztonságimásolat-fájl mappájához és fájlnevéhez, majd kattintson vagy koppintson a **Megnyitás** gombra. **3.** Adja meg a jelszót, melyet a biztonsági mentés közben készített.

- **Névjegy**—Megjelenik a Trust Circle Manager/Reader szoftververziója. Megjelennek a hivatkozások, hogy lehetővé tegyék a Trust Circle Manager Pro verzióra frissítését vagy megjelenjen a HP adatvédelmi nyilatkozata.

9 Lopás helyreállítása (csak bizonyos modelleknél)

A Computrace (külön vásárolható) lehetővé teszi, hogy távolról figyelje, kezelje és nyomon kövesse a számítógépét.

Amikor aktiválta, a Computrace az Absolute Software Customer Center-ből kerül konfigurálásra. A Customer Center-ben a rendszergazda konfigurálhatja a Computrace-t, hogy figyelje vagy kezelje a számítógépet. Ha a rendszer eltűnik vagy azt ellopják, a Customer Center segítheti a helyi hatóságokat a számítógép helyének meghatározásában és felfedezésében. Ha konfigurált, a Computrace folytathatja a máködését még akkor is, ha a merevlemezt letörölték vagy kicserélték.

A Computrace aktiválásához:

1. Csatlakozzon az internethez.
2. Nyissa meg a HP Client Security alkalmazást. További információ itt olvasható: A HP Client Security megnyitása, 10. oldal.
3. Kattintson a **Theft Recovery** alkalmazásra.
4. A Computrace aktiválásvarázsló elindításához kattintson a **Kezdés** opcióra.
5. Adja meg az elérhetőségeit és a hitelkártya fizetési adatait, vagy adjon meg egy előre megvásárolt termékkulcsot.

Az aktiválásvarázsló feldolgozza a tranzakciót és beállítja a felhasználói fiókját az Absolute Software Customer Center weboldalon. Amint készen van, megerősítő e-mailt kap, mely tartalmazza a Customer Center fiókadatait.

Ha korábban futtatta a Computrace aktiválásvarázslót és még megvan a Customer Center felhasználói fiókja, akkor vásárolhat további linecszeket, ha a HP fiókképviselőjéhez fordul.

A Customer Center-be való bejelentkezéshez:

1. Keresse fel a https://cc.absolute.com/ címet.
2. A **Bejelentkezési azonsoító** és a **Jelszó** mezőkben adja meg a hitelesítő adatokat, melyeket a megerősítő e-mailben kapott, majd kattintson a **Bejelentkezés** lehetőségre.

A Customer Center segítségével:

- Figyelheti a számítógépeit.
- Megvédheti a távoli adatait.
- Bármely, Computrace által védett számítógép lopását bejelentheti.

▲ Kattintson a **További információk** lehetőségre, hogy többet tudjon meg a Computrace alkalmazásról.

10 Lokalizált jelszókivételek

A rendszerindításkori hitelesítés szintjén és a HP Drive Encryption szintjén a jelszólokalizálás támogatása korlátozott. További információ itt olvasható: A rendszerindításkori hitelesítés szintjén vagy a Drive Encryption szinten nem támogatott Windows IME-k, 56. oldal.

Mi a teendő jelszó visszautasításakor

A jelszók az alábbi okok miatt kerülhetnek visszautasításra:

- Egy felhasználó nem támogatott IME-t használ. Ez gyakori probléma a két bites nyelvek esetében (koreai, japán, kínai). A probléma megoldásához:

  1. A **vezérlőpulton** adjon meg támogatott billentyűzetkiosztást (adja hozzá a kínai beviteli nyelvhez a US/angol billentyűzetet).
  2. Állítsa be a támogatott billentyűzetet az alapértelmezett bevitelhez.
  3. Indítsa el a HP Client Security programot, majd adja meg a Windows-jelszót.

- Egy felhasználó nem támogatott karaktert használ. A probléma megoldásához:

  1. Módosítsa úgy a Windows-jelszót, hogy csak támogatott karaktereket használjon. A nem támogatott karakterekkel kapcsolatos további információ: Speciális billentyűk kezelése, 57. oldal.
  2. Indítsa el a HP Client Security programot, majd adja meg a Windows-jelszót.

A rendszerindításkori hitelesítés szintjén vagy a Drive Encryption szinten nem támogatott Windows IME-k

A Windows-ban a felhasználó választhat egy IME-t (beviteli mód szerkesztője), hogy komplex karaktereket és szimbólumokat adjon meg (például japán vagy kínai karakterek) a normál nyugati billentyűzet segítségével.

A rendszerindításkori hitelesítés szintjén vagy a Drive Encryption szinten nem támogatottak az IME-k. IME-vel nem adható meg Windows jelszó a rendszerindításkori hitelesítés vagy a HP Drive Encryption bejelentkező képernyőn, és ha így tesz azzal kizárásos helyzetet kaphat. Néhány esetben a Microsoft® Windows nem jeleníti meg az IME-t, amikor a felhasználó megadja a jelszót.

A megoldás átkapcsolni az alábbi támogatott billentyűzetkiosztásra, mely lefordítja a 00000411 billentyűzetkiosztást.

- Microsoft IME japán esetén
- A japán billentyűzetkiosztás
- Office 2007 IME japán esetén—Ha a Microsoft vagy haremadik fél az IME vagy beviteli mód szerkesztője fogalmat használ, a beviteli mód lehet, hogy valójában nem IME. Ez keveredést okozhat, de a szoftver olvassa a hexadecimális kód képviselőjét. Tehát ha egy támogatott billentyűzetkiosztás feltérképezi az IME-t, akkor a HP Client Security támogatni tudja a konfigurációt.

FIGYELEM! Amikor a HP Client Security telepített, a Windows IME-vel megadott jelszavak elutasításra kerülnek.

A támogatott billentyűzetkiosztás segítségével történő jelszómódosítások

Ha a jelszót egy billentyűzetkiosztással állították először be (például U.S. English (409)), és akkor a felhasználó másik billentyűzetkiosztással megváltoztatja a jelszót, mely szintén támogatott (például Latin American (080A)), akkor a jelszómódosítás a HP Drive Encryption programban működik, de nem sikerül a BIOS-ban, ha a felhasználó olyan karaktereket használ, melyek jelen vannak az utóbbiban, de nem léteznek az előbbiben (például: ē).

MEGJEGYZÉS: A rendszergazdák megoldhatják ezt a problémát ha a HP Client Security felhasználók oldalát használják (melyet a kezdőlap **fogaskerék** ikonjáról ér el), hogy eltávolítsák a felhasználót a HP Client Security programból, kiválasztva a kívánt billentyűzetkiosztást az operációs rendszerben, majd futtatva a HP Client Security telepítő varázslót ismét ugyanahhoz a felhasználóhoz. A BIOS tárolja a kívánt billentyűzetkiosztást, és az ezen billentyűzetkiosztással begépelhető jelszavak megfelelően lesznek beállítva a BIOS-ban.

Egy másik lehetséges probléma a különböző billentyűzetkiosztás használata, melyek mindegyike ugyanazon karaktereket adja. Például a U.S. International keyboard layout (20409) és a Latin American keyboard layout (080A) egyaránt adja az é karaktert, de különböző billentyű lenyomási sorrendre lehet szükség. Ha egy jelszót először a Latin American keyboard layout billentyűzetkiosztással állítottak be, akkor a Latin American keyboard layout kerül beállításra a BIOS-ban, még akkor is, ha a jelszót később a U.S. International keyboard layout billentyűzetkiosztással módosítják.

Speciális billentyűk kezelése

- Kínai, szlovák, kanadai francia és cseh

  Amikor egy felhasználó az egyik korábbi billentyűzetelrendezést választja ki, majd megad egy jelszót (például: abcdef), akkor ugyanazt a jelszót kell megadni, miközben nyomva tartja a shift billentyűt kisbetű esetén, és a shift billentyűt és a caps lock billentyűt a felső esetben a Power-on authentication és HP Drive Encryption esetén. A numerikus jelszavakat a numerikus billentyűzettel kell megadni.

- Koreai

  Amikor egy felhasználó egy támogatott koreai billentyűzetelrendezést választ ki, majd megad egy jelszót, akkor ugyanazt a jelszót kell megadni, miközben nyomva tartja a jobb oldali alt billentyűt kisbetű esetén, és a jobb oldali alt billentyűt és a caps lock billentyűt a felső esetben a Power-on authentication és HP Drive Encryption esetén.

- A nem támogatott karakterek az alábbi táblázatban találhatók:

Language (Nyelv)	Windows	BIOS	Drive Encryption
Arab	A ﻻ ,ﻷ, és ﻹ billentyűk két karaktert generálnak.	A ﻻ ,ﻷ, és ﻹ billentyűk egy karaktert generálnak.	A ﻻ ,ﻷ, és ﻹ billentyűk egy karaktert generálnak.
Kanadai francia	ç, è, à és é a caps lock billentyűvel Ç, È, À és É lesz a Windows-ban.	ç, è, à és é a caps lock billentyűvel ç, è, à és é lesz a Power-in authentication esetén	ç, è, à és é a caps lock billentyűvel ç, è, à és é lesz a HP Drive Encryption esetén

Language (Nyelv)	Windows	BIOS	Drive Encryption
Spanyol	A 40a nem támogatott. Működik azonban, mivel a szoftver átalakítja c0a-vá. A billentyűzetkiosztások közötti finom különbségek miatt azonban javasolt a spanyolul beszélő felhasználóknak módosítaniuk a Windows billentyűzetkiosztásukat az 1040a Spanish Variation) vagy 080a (Latin American) billentyűzetkiosztásra változtatniuk.	n/a	n/a
US international	◦ A sor tetején a ¡, ¤, ‘, ’, ¥ és × billentyűk elutasítottak. ◦ A második sorban a å, ® és Þ billentyűk elutasítottak. ◦ A harmadik sorban a á, ð és ø billentyűk elutasítottak. ◦ Az alsó sorban a æ billentyű elutasított.	n/a	n/a
Cseh	◦ A ğ billentyű elutasított. ◦ A į billentyű elutasított. ◦ A ų billentyű elutasított. ◦ Az ė, ı és ż billentyűk elutasítottak. ◦ A ģ, ķ, ļ, ņ és ţ billentyűk elutasítottak.	n/a	n/a
Szlovák	A ż billentyű elutasított.	◦ Gépelve az š, ś és ş billentyűk elutasítottak, de elfogadottak, amikor változtatható billentyűzettel adják meg. ◦ A ţ holt billentyű két karaktert generál.	n/a
Magyar	A ż billentyű elutasított.	A ţ billentyű két karaktert generál.	n/a
Szlovén	A żŻ billentyű elutasított a Windowsban, az alt billentyű pedig holt billentyűt generál a BIOS-ban.	Az ú, Ú, ů, Ů, ş, Ş, ś, Ś, š és Š billentyűk elutasítottak a BIOS-ban.	n/a
Japán	Ahol lehet, a Microsoft Office 2007 IME a legjobb választás. Az IME neve ellenére valójában 411-es billentyűzetkiosztás, amely támogatott.	n/a	n/a

Szójegyzék

aktiválás
Az a feladat, amelyet bármilyen Drive Encryption funkció elérése előtt el kell végezni. A rendszergazdák aktiválhatják a Drive Encryption szoftvert a HP Client Security telepítő varázslóban vagy a HP Client Security programban. Az aktiválási folyamat a szoftver aktiválásából, a meghajtó titkosításából és az első biztonsági mentési titkosítási kulcs létrehozásából áll a cserélhető tárolóeszközön.

automatikus foszlatás
A File Sanitizer-ben ütemezett megsemmisítés.

Azonosítókártya
A Windows asztal arra szolgál, hogy vizuálisan azonosítsa az asztalát a felhasználónevével és a kiválasztott képpel.

bejelentkezés
Olyan objektum a HP Client Security programon belül, mely felhasználónévből és jelszóból áll (és esetleg más kiválasztott adatokból), melyek weboldalakra vagy más programokba való bejelentkezéshez használhatók.

biztonsági bejelentkezési eljárás
A számítógépbe való bejelentkezéshez használt eljárás.

biztonsági mentés
A biztonsági mentési szolgáltatás használata fontos programadatok másolatának mentésére programon kívüli helyre. Később használható az adatok visszaállítására ugyanarra a számítógépre vagy egy másikra.

Bluetooth
Olyan technológia, mely rádiójeleket használt Bluetooth-kompatibilis számítógépek, nyomtatók, egerek, mobiltelefonok és más készülékek vezeték nélküli kommunikációjához rövid távolságon belül.

csatlakoztatott eszköz
A számítógép egy portjához csatlakoztatott hardvereszköz.

csoport
Felhasználók csoportja, akiknek azonos szintű a hozzáférésük vagy egy eszközosztályhoz vagy egy adott eszközhöz nincs hozzáférésük.

dekódolás
Olyan eljárás, melyet a kriptográfiában használnak a titkosított adatok sima szöveggé alakításához.

Drive Encryption
A merevlemez(ek) titkosításával védi meg az adatokat, mivel az engedély nélküli felhasználók nem tudják őket elolvasni.

Drive Encryption bejelentkezési képernyő
Lásd: Drive Encryption rendszerindítás előtti hitelesítés

Drive Encryption rendszerindítás előtti hitelesítése
Olyan bejelentkezési képernyő, amely a Windows indítása előtt jelenik meg. A felhasználóknak meg kell adniuk a Windows felhasználói nevüket és jelszavukat, vagy az intelligens kártya PIN-kódját, vagy le kell húzniuk egy regisztrált ujjukat. Ha az egylépéses bejelentkezést választja, akkor a Drive Encryption bejelentkezési képernyőjén megadva a helyes adatokat közvetlen hozzáférése lesz a Windows-hoz anélkül, hogy ismét be kellene jelentkeznie a Windows bejelentkezési képernyőn.

DriveLock

Olyan biztonsági funkció, mely a merevlemezt egy felhasználóhoz köti, és melynél a felhasználónak helyesen kell begépelnie a DriveLock jelszót, amikor a számítógép elindul.

Egyszeri bejelentkezés
Olyan funkció, mely a hitelesítő adatokat tárolja, és lehetővé teszi, hogy a HP Client Security alkalmazást használja az Internet és a Windows alkalmazások eléréséhez, melyekhez jelszavas hitelesítés szükséges.

érintkezés nélküli kártya
Számítógép-chipet tartalmazó műanyag kártya, mely hitelesítésre használható.

erőforrás
Személyes adatokat vagy fájlokat tartalmazó adatkomponens, előzmény- és webbel kapcsolatos adatok stb., melyek a merevlemezen találhatók.

eszközhozzáférés-szabályozási házirend
Azon eszközök listája, melyhez egy felhasználó hozzáférése engedélyezett vagy sem.

eszközosztály
Egy adott típusú összes eszköz, például meghajtók.

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
Olyan algoritmus futtatása, mely az elemben található adatokat jelentés nélküli adatokkal írja felül.

hálózati fiók
Windows felhasználói vagy rendszergazdai fiók vagy a helyi számítógépen, munkacsoportban, vagy egy doménen.

hardvertitkosítás
Az öntitkosító meghajtók kezelésére vonatkozó Trusted Computing Group OPAL jellemzőinek megfelelő öntitkosító meghajtók használata az azonnali titkosítás elvégzéséhez. A hardvertitkosítás azonnali és csak néhány percig tart, míg a szoftvertitkosítás több órát is igénybe vehet.

hitelesítés
Az a folyamat, mely hitelesítő adatok (Windows-jelszó, ujjlenyomat, intelligens kártya, érintkezés nélküli kártya vagy közelségérzékelő kártya) segítségével megerősíti, hogy Ön az a személy, aki.

hitelesítő adat
Egy adott információ vagy hardvereszköz, mely adott felhasználó hitelesítésére használatos.

HP SpareKey helyreállítás
A számítógép elérésének lehetősége a biztonsági kérdésekre helyes választ adva.

identitás
A HP Client Security-ban hitelesítő adatok és beállítások csoportja, melyeket fiókként vagy profilként kezelnek adott felhasználó esetén.

intelligens kártya
Olyan hardvereszköz, mely PIN-kóddal használatos hitelesítésre.

Kezdőlap
Olyan központi hely, ahol elérheti és kezelheti a funkciókat és beállításokat a HP Client Security programban.

közelségérzékelő kártya
Számítógép-chipet tartalmazó műanyag kártya, mely hitelesítésre használatos más hitelesítő adatokkal együtt a további biztonság érdekében.

manuális foszlatás

Elem vagy kiválasztott elemek azonnali megsemmisítése, mely kikerül egy ütemezett megsemmisítést.

PIN-kód
Regisztrált felhasználók személyi azonosítószáma, mely hitelesítésre használatos.

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

Pont időben hitelesítés
Lásd a HP eszközhozzáférés-kezelő szoftver súgóját.

rendszergazda
Lásd: *Windows rendszergazda*.

rendszerindításkori hitelesítés
Olyan biztonsági funkció, mely a hitelesítés néhány formáját igényli, amikor a számítógép bekapcsol; ilyenek az intelligens kártya, a biztonsági chip vagy a jelszó..

szabad lemezterület teljes törlése
Véletlen adatok írása a törölt elemekre és nem hasznát területekre. Ez a folyamat csökkenti a törölt elemek létét úgy, hogy az eredeti elem helyreállítása nehezebb.

szoftvertitkosítás
Szoftver használata a merevlemez titkosításához szektorról szektorra. Ez a folyamat lassabb, mint a hardvertitkosítás.

tartomány
Számítógépek csoportja, mely egy hálózat része és megosztja a szokásos mappa-adatbázist. A domének nevei egyediek, és mindegyiknek vannak szokásos szabályai és eljárásai.

titkosítás
Algortimushoz hasonló eljárást alkalmaznak a kriptográfiában a sima szöveg rejtett szöveggé alakításához, hogy megakadályozzák az engedéllyel nem rendelkezők számára az adatok elolvasását. Sokféle adattitkosítási típus létezik, a hálózati biztonság alapjai ezek. A szokásos típusok a Data Encryption Standard és a nyilvános kulcs titkosítás.

titkosított fájlrendszer (EFS)
Olyan rendszer, mely az összes fájlt és almappát titkosítja a kiválasztott mappában.

Trust Circle
Adatok elszigetelését biztosítja, mivel az adatokat meghatározott, megbízható felhasználókhoz köti. Ez megakadályozza, hogy véletlenül vagy szándékosan rossz kezekbe kerüljenek az adatok. A CryptoMill’s Zero Overhead Key Management technológia biztosítja, az adatok kriptografikusan kötődnek a bizalmi körhöz. Ez megakadályozza dokumentumok vagy más érzékeny adatok visszafejtését a bizalmi körön kívül.

Trust Circle Manager/Reader
A Trust Circle Reader csak a Trust Circle Manager felhasználói által kiküldött meghívásokat fogadja el. A Trust Circle Manager azonban lehetővé teszi Trust Circles létrehozását. A funkciók közé tartozik valaki meghívása e-mailben egy Trust Circle-be és mások Trust Circle meghívásainak elfogadása. Amint létrehoztak egy Trust Circle-t egyenrangú felek között, a Trust Circle által védett fájlok biztonságosan megoszthatók.

Trust Circle mappa
Minden Trust Circle-lel védett mappa.

Trusted Platform Module (TPM) beágyazott biztonsági chip
Egy TPM hitelesíti egy számítógépet, és nem egy felhasználó, azzal, hogy a gazdarendszerre specifikus információkat tárol, például titkosítási kulcsokat, digitális tanúsítványokat és jelszavakat. Egy TPM minimálisra csökkenti annak lehetőségét, hogy a számítógépen található információk kompromittáltak legyenek fizikai lopás vagy külső hacker támadása miatt.

ujjlenyomat
Ujjelnyomata képének digitális kivonata. A tényleges ujjlenyomatképe sosem kerül tárolásra a HP Client Security-ben.

újraindítás
A számítógép újraindítási folyamata

vész-helyreállítási archívum
Védett tárolóterület, mely lehetővé teszi az Alap felhasználói kulcsok újratitkosítását az egyik platform tulajdonosának kulcsáról egy másikhoz.

visszaállítás
Olyan folyamat, mely a programinformációkat egy korábban mentett biztonságimásolat-fájlból ebbe a programba másolja.

Windows bejelentkezési biztonság
Védi a Windows fiók(ok) védelmét, mivel adott hitelesítési adatokat kér a belépéshez.

Windows felhasználói fiók
Olyan felhasználó, aki bejelentkezhet egy hálózatra vagy egy adott számítógépre.

Windows rendszergazda
Teljes jogú felhasználó engedélyek módosításához és más felhasználók kezeléséhez.

Tárgymutató