HP Client Security

Noţiuni introductive

Prima ediţie: August 2013

Cod document: 735339-271

Cuprins

1 Introducere HP Client Security Manager

HP Client Security vă permite să vă protejați datele, dispozitivul și identitatea, îmbunătățindu-vă astfel securitatea computerului dvs.

Modulele de software disponibile pentru computerul dvs. pot varia în funcţie de modelul dvs.

Modulele de software HP Client Security pot fi preinstalate, preîncărcate sau disponibil pentru descărcare de pe site-ul web HP. Pentru mai multe informaţii, consultaţi http://www.hp.com.

NOTĂ: Instrucţiunile din acest ghid sunt scrise cu presupunerea că aţi instalat deja modulele software HP Client Security adecvate.

Caracteristici HP Client Security

Tabelul următor detaliază principalele caracteristicile ale modulelor HP Client Security.

Modul	Caracteristici principale
HP Client Security Manager	Administratorii pot efectua următoarele funcţii: • Protejaţi-vă computerul înainte de pornirea sistemului de operare Windows® • Pentru a vă proteja contul Windows folosind o autentificare puternică • Pentru a vă gestiona datele de conectare și parolele aferente anumitor site-uri web și aplicații • Schimbaţi cu uşurinţă parola sistemului de operare Windows • Folosiți amprentele pentru mai multă securitate și confort • Configurați un smart card, un card fără contact sau un card de proximitate pentru autentificare • Folosiți-vă telefonul prevăzut cu Bluetooth ca metodă de identificare • Configurați un PIN pentru a vă extinde soluțiile de autentificare • Configurați-vă politicile de conectare și de sesiune • Efectuați copii de rezervă și restaurați-vă datele de program • Adăugați mai multe aplicații, precum HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager și HP Computrace Utilizatorii generali pot efectua următoarele funcţii: • Vizualizaţi setările pentru Stare de criptare şi Device Access Manager. • Activaţi Computrace. • Configuraţi Preferinţe, Copiere de rezervă şi Restaurare opţiuni.

Modul	Caracteristici principale
Password Manager	Utilizatorii generali pot efectua următoarele funcţii: • Organizaţi şi configuraţi numele de utilizator şi parolele. • Creaţi parole mai puternice pentru o securitate îmbunătăţită a conturilor de e-mail şi a conturilor Web. Password Manager completează şi trimite informaţiile în mod automat. • Eficientizaţi procesul de conectare folosind caracteristica Single Sign On, care reţine şi aplică automat acreditările utilizatorului. • Marcaţi un cont ca fiind compromis, astfel încât să fiţi avertizat pentru alt(e) cont(uri) cu acreditări similare. • Importaţi datele de conectare dintr-un browser acceptat.
HP Drive Encryption (numai la anumite modele)	• Oferă o criptare completă de volum a unităţii de disc. • Forţează autentificarea prealabilă încărcării pentru a decripta şi pentru a accesa datele. • Oferă opţiunea de a activa unităţile cu criptare automată (numai la anumite modele).
HP Device Access Manager	• Permite administratorilor IT să controleze accesul la dispozitivele bazate pe profiluri de utilizator. • Împiedică utilizatorii neautorizaţi să elimine datele cu ajutorul unui suport media de stocare extern şi să introducă viruşi în sistem de pe suportul media extern. • Permite administratorilor să dezactiveze accesul la dispozitive de comunicaţii pentru anumite persoane sau grupuri de utilizatori.
HP Trust Circles	• Oferă securitatea fişierelor şi documentelor. • Criptează fişierele plasate în folderele specificate de utilizator şi le protejează în cadrul unui circuit al încrederii. • Permite utilizarea şi partajarea fişierelor exclusiv de către membrii aflaţi în circuitul de încredere.
Theft Recovery (Recuperare furt) (Computrace, cumpărat separat)	• Pentru activare, necesită cumpărarea separată a abonamentelor de depistare şi urmărire. • Oferă urmărirea securizată a datelor. • Monitorizează activitatea utilizatorilor, precum şi modificările hardware şi software. • Rămâne activ chiar dacă unitatea de disc este reformatată sau înlocuită.

Descrierea produsului HP Client Security şi exemple de utilizare obişnuite

Majoritatea produselor HP Client Security deţin atât metoda de autentificare cu utilizator (de obicei o parolă) cât şi o alternativă administrativă de a avea acces atunci când parolele sunt pierdute, sunt indisponibile, sunt uitate sau de fiecare dată când persoanele responsabile cu securitatea firmei solicită accesul.

NOTĂ: Unele dintre produsele HP Client Security sunt concepute pentru a restricţiona accesul la date. Datele trebuie criptate, atunci când pentru utilizator este mai important să piardă informaţiile decât să ii fie compromise. Se recomandă ca toate datele să fie copiate de rezervă într-un loc sigur.

Password Manager

Password Manager stochează nume de utilizator şi parole şi poate fi utilizat pentru:

- Salvaţi nume de conectare şi parole pentru acces la Internet sau e-mail.
- Conectaţi automat utilizatorul la un site Web sau la E-mail.
- Gestionaţi şi organizaţi autentificările.
- Selectaţi date Web sau de reţea şi accesaţi direct legătura.
- Vizualizarea numelor şi parolelor atunci când este necesar.
- Marcaţi un cont ca fiind compromis, astfel încât să fiţi avertizat pentru alt(e) cont(uri) cu acreditări similare.
- Importaţi datele de conectare dintr-un browser acceptat.

Exemplul 1: Un agent de cumpărări al unui mare producător efectuează majoritatea tranzacţiilor firmei pe Internet. Ea vizitează frecvent mai multe Site-uri Web cunoscute care solicită informaţii de conectare. Ea este perfect conştientă de regulile privind securitatea şi nu utilizează aceeaşi parolă pentru fiecare cont. Agentul de cumpărări a decis să utilizeze Password Manager pentru a corela legăturile Web cu diferite nume de utilizator şi parole. Atunci când accesează un site Web pentru a se conecta, Password Manager oferă acreditările în mod automat. Dacă doreşte să vizualizeze numele de utilizator şi parolele, Password Manager poate fi configurat pentru a le afişa.

Password Manager poate fi utilizat de asemenea pentru a administra şi a organiza autentificări. Acest instrument va permite unui utilizator să selecteze date Web sau de reţea şi să acceseze direct legătura. Atunci când este necesar, utilizatorul poate de asemenea să vizualizeze numele de utilizator şi parolele.

Exemplul 2: Un angajat harnic a fost promovat şi va conduce de acum întreg departamentul de contabilitate. Echipa trebuie să se conecteze la un număr mare de conturi de client Web şi fiecare dintre acestea utilizează informaţii de conectare diferite. Aceste informaţii de conectare trebuie partajate cu alţi angajaţi, prin urmare, confidenţialitatea devine o problemă. Angajatul decide să organizeze toate legăturile Web, numele de utilizator din companie şi parolele în cadrul Password Manager. După finalizare, angajatul le prezintă angajaţilor Password Manager, pentru ca aceştia să lucreze pe conturi Web fără să cunoască niciodată acreditările de conectare pe care le utilizează.

HP Drive Encryption (numai la anumite modele)

HP Drive Encryption este folosită pentru a restricţiona accesul la datele de pe întreaga unitate de disc a computerului sau de pe o unitate secundară. Drive Encryption poate administra de asemenea unităţile cu criptare automată.

Exemplul 1: Un medic doreşte să se asigure că numai el poate accesa orice date de pe unitatea de disc a computerului. Medicul activează Drive Encryption, care necesită autentificarea prealabilă încărcării înainte de conectarea la Windows. După configurare, unitatea de disc nu mai poate fi accesată fără o parolă înainte de pornirea sistemului de operare. Medicul poate îmbunătăţi suplimentar securitatea unităţii prin alegerea criptării datelor cu opţiunea unitate cu criptare automată.

Exemplul 2: Un administrator de spital doreşte să se asigure că numai doctorii şi personalul autorizat pot accesa orice date de pe computerele lor fără să partajeze parolele personale. Departamentul IT adaugă administratorul, doctorii şi întreg personalul autorizat ca utilizatori Drive Encryption. Acum,

numai personalul autorizat poate porni computerul sau domeniul folosind numele de utilizator şi parola personale.

HP Device Access Manager (numai la anumite modele)

HP Device Access Manager permite unui administrator să restricţioneze şi să gestioneze accesul la hardware. Device Access Manager poate fi utilizat pentru blocarea accesului neautorizat la unităţile flash USB în care pot fi copiate date. De asemenea, acesta poate restricţiona accesul la unităţile CD/DVD, poate verifica dispozitivele USB, conexiunile de reţea, ş.a.m.d. Un exemplu ar fi situaţia în care furnizori externi sunt nevoiţi să acceseze computerele companiei, dar fără să poată copia date pe o unitate USB.

Exemplul 1: Administratorul unei companii de echipamente medicale intră adesea în contact cu fişe medicale personale şi informaţii despre companie. Angajaţii trebuie să acceseze aceste date, cu toate acestea, este foarte important ca datele să nu fie scoase din computer printr-o unitate USB sau orice alt suport media de stocare. Reţeaua este sigură, dar computerele sunt dotate cu inscriptoare de CD-uri şi porturi USB care pot permite copierea sau furtul datelor. Administratorul utilizează Device Access Manager pentru a dezactiva porturile USB şi inscriptoarele de CD-uri, pentru ca acestea să nu poată fi utilizate. Chiar dacă porturile USB sunt blocate, mouse-ul şi tastaturile vor continua să funcţioneze.

Exemplul 2: O societate de asigurări nu doreşte ca angajaţii să instaleze sau să încarce software personal sau date provenite de acasă. Anumiţi angajaţi trebuie să acceseze portul USB de pe toate computerele. Administratorul IT utilizează Device Access Manager pentru a permite accesul anumitor angajaţi, în timp ce blochează accesul extern pentru alţii.

Computrace (cumpărat separat)

Computrace (cumpărat separat) este un serviciu care poate urmări locaţia unui computer furat atunci când utilizatorul accesează Internet-ul. De asemenea, Computrace poate ajuta la administrarea şi localizarea de la distanţă a computerelor, precum şi la monitorizarea utilizării computerului şi a aplicaţiilor.

Exemplul 1: Directorul unei şcoli a solicitat departamentului IT să monitorizeze toate computerele din şcoală. După inventarierea computerelor, administratorul IT a înregistrat toate computerele cu Computrace, pentru ca acestea să poată fi urmărite în cazul în care au fost furate. De curând, angajaţii şcolii au descoperit lipsa mai multor computere, prin urmare, administratorul IT a alertat autorităţile şi persoanele responsabile cu Computrace. Computerele au fost localizate şi returnate şcolii de către autorităţile competente.

Exemplul 2: O companie imobiliara doreşte să îşi administreze şi actualizeze computerele din întreaga lume. Aceştia utilizează Computrace pentru a monitoriza şi a actualiza computerele fără să trimită o persoană la fiecare computer.

Atingerea obiectivelor principale privind securitatea

Modulele HP Client Security pot conlucra pentru a oferi soluţii pentru o varietate de probleme privind securitatea, inclusiv următoarele obiective principale privind securitatea:

- Protecţia împotriva furturilor plănuite
- Restricţionarea accesului la date confidenţiale
- Împiedicarea accesului neautorizat din locaţii interne sau externe
- Crearea de reglementări în vigoare privind parola puternică

Protecţia împotriva furturilor plănuite

Un exemplu de furt plănuit ar fi furtul unui computer aflat în punctul de control dintr-un aeroport, ce conţine date confidenţiale şi informaţii despre clienţi. Următoarele caracteristici ajută la protecţia împotriva furtului plănuit:

- Dacă este activată, caracteristica de autentificare prealabilă încărcării, ajută la împiedicarea accesului la sistemul de operare.
  - HP Client Security—Consultaţi HP Client Security, la pagina 12.
  - HP Drive Encryption—Consultaţi HP Drive Encryption (numai la anumite modele), la pagina 30.
- Criptarea vă asigură că datele nu pot fi accesate chiar dacă unitatea de disc este îndepărtată şi instalată într-un sistem nesecurizat.
- După ce a fost furat, Computrace poate urmări locaţia computerului.
  - Computrace—Consultaţi Theft Recovery (Recuperare furt) (numai la anumite modele), la pagina 54.

Restricţionarea accesului la date confidenţiale

Să presupunem că un revizor contabil îşi desfăşoară activitatea la sediul clientului şi că a primit accesul la un computer pentru a analiza date financiare confidenţiale. Dvs. nu doriţi ca revizorul contabil să poată imprima sau salva fişierele pe un dispozitiv pe care se poate scrie, precum un CD. Următoarea caracteristică vă ajută să restricţionaţi accesul la date:

- HP Device Access Manager permite administratorilor IT să restricţioneze accesul la dispozitive de comunicaţii pentru ca informaţiile confidenţiale să nu poată fi copiate din unitatea de disc. Consultaţi Vizualizare sistem, la pagina 44.

Împiedicarea accesului neautorizat din locaţii interne sau externe

Accesul neautorizat la un computer nesecurizat pentru afaceri prezintă un adevărat risc pentru resursele din reţeaua de întreprindere, precum informaţiile provenite de la serviciile financiare, un director sau de la echipa de cercetare şi dezvoltare şi pentru informaţiile private cum precum fişele pacienţilor sau registrele financiare ale angajaţilor. Următoarele caracteristici ajută la împiedicarea accesului neautorizat:

- Dacă este activată, caracteristica de autentificare prealabilă încărcării, ajută la împiedicarea accesului la sistemul de operare. (consultaţi HP Drive Encryption (numai la anumite modele), la pagina 30.
- HP Client Security vă asigură că un utilizator neautorizat nu poate obţine parole şi nu poate accesa aplicaţiile protejate prin parolă. Consultaţi HP Client Security, la pagina 12.
- HP Device Access Manager permite administratorilor IT să restricţioneze accesul la dispozitive pe care se poate scrie pentru ca informaţiile confidenţiale să nu poată fi copiate din unitatea de disc. Consultaţi HP Device Access Manager (numai la anumite modele), la pagina 43.

Crearea de reglementări în vigoare privind parola puternică

Dacă politica unei companiei intră în vigoare şi solicită utilizarea de reglementări în vigoare privind parola puternică pentru zeci de aplicaţii şi baze de date aflate pe Web, Password Manager oferă un depozit protejat pentru parole şi facilitatea Single Sign On. Consultaţi Password Manager, la pagina 18.

Elementele suplimentare de securitate

Alocarea rolurilor de securitate

În gestionarea securităţii computerului (în special pentru organizaţiile mari), una dintre cele mai importante reguli este repartizarea responsabilităţilor şi drepturilor între diferitele tipuri de administratori şi utilizatori.

NOTĂ: Într-o organizaţie mică sau pentru utilizarea individuală, aceste roluri pot fi deţinute de către aceeaşi persoană.

Pentru HP Client Security, obligaţiile şi privilegiile privind securitatea se împart în următoarele roluri:

- Funcţionarul securitate-Defineşte nivelul de securitate al companiei sau al reţelei şi determină caracteristicile de securitate ce trebuie implementate, precum Drive Encryption.

  NOTĂ: Multe dintre caracteristicile din HP Client Security pot fi personalizate de către funcţionarul securitate în colaborare cu HP. Pentru mai multe informaţii, consultaţi http://www.hp.com.

- Administratorul IT-Aplică şi gestionează caracteristicile de securitate definite de către funcţionarul securitate. De asemenea, acesta poate activa şi dezactiva anumite caracteristici. De exemplu, dacă funcţionarul securitate a decis să implementeze smart carduri, administratorul IT poate activa atât modul parolă cât şi modul smart card.

- Utilizatorul-Foloseşte caracteristicile de securitate. De exemplu, dacă funcţionarul securitate şi administratorul IT au activat smart carduri pentru sistem, utilizatorul poate seta PIN-ul pentru smart card şi poate utiliza cardul pentru autentificare.

ATENŢIE: Administratorii sunt încurajaţi să urmeze "cele mai bune practici" în restricţionarea privilegiilor utilizatorului final şi în restricţionarea accesului utilizatorului.

Utilizatorii neautorizaţi nu trebuie să primească privilegii administrative.

Gestionarea parolelor HP Client Security

Majoritatea caracteristicilor HP Client Security sunt protejate prin parole. Tabelul următor listează cele mai des folosite parole, modulul de software în care este setată parola şi funcţia parolei.

Parolele setate şi utilizate numai de către administratorii IT sunt indicate de asemenea în acest tabel. Toate celelalte parole pot fi setate de către utilizatori sau administratori obişnuiţi.

Parolă HP Client Security	Setaţi în următorul modul	Funcţie
Parolă conectare Windows	Panoul de control Windows sau HP Client Security	Poate fi utilizat pentru conectare manuală şi pentru autentificare cu scopul de a accesa diferitele caracteristici HP Client Security.
Copierea de rezervă şi recuperarea parolei HP Client Security	HP Client Security, de către utilizatorul individual	Protejează accesul la Copierea de rezervă şi recuperarea fişierului HP Client Security.
PIN pentru smart card	Credential Manager	Poate fi folosit ca autentificare multifactorială. Poate fi folosit ca autentificare Windows. Autentifică utilizatorii de Drive Encryption, dacă este selectat smart cardul.

Crearea unei parole securizată

Atunci când creaţi parole, trebuie să urmaţi în prealabil orice specificaţii care au fost setate de către program. În general, luaţi în considerare următoarele instrucţiuni care vă ajuta să creaţi parole puternice şi să reduceţi şansele ca parola dvs. să fie compromisă:

- Utilizaţi parole mai lungi de 6 caractere, de preferinţă mai lungi de 8.
- Amestecaţi în parolă literele mari cu cele mici.
- Atunci când este posibil, amestecaţi caractere alfanumerice şi includeţi caractere speciale şi semne de punctuaţie.
- Înlocuiţi caracterele speciale sau numerele cu litere pentru a forma un cuvânt cheie. De exemplu, în locul de numărul 1 puteţi folosi literele I sau L.
- Combinaţi cuvinte din 2 sau mai multe limbi.
- Împărţiţi la mijloc un cuvânt sau o frază cu numere sau caractere speciale, de exemplu, "Mary2-2Cat45".
- Nu utilizaţi o parolă care poate apărea în dicţionar.
- Nu utilizaţi numele dvs. ca parolă sau orice alte informaţii personale, precum data naşterii, nume de animale de companie sau numele de domnişoară al mamei dvs. chiar dacă le scrieţi invers.
- Schimbaţi parolele în mod regulat. Pentru a spori siguranţa, modificaţi doar câteva caractere.
- Dacă notaţi parola, nu o lăsaţi într-un loc vizibil aflat în apropierea computerului.
- Nu salvaţi parola într-un fişier, precum un e-mail, pe computer.
- Nu partajaţi conturi şi nu comunicaţi nimănui parola.

Copierea de rezervă a acreditărilor şi setărilor

Puteţi utiliza instrumentul Copiere de rezervă şi recuperare din HP Client Security ca locaţie centrală din care puteţi efectua copii de siguranţă şi puteţi restaura acreditările de securitate de la unele module HP Client Security.

2 Noţiuni introductive

Pentru a configura HP Client Security astfel încât să funcționeze cu acreditările dvs., lansați HP Client Security într-unul din următoarele moduri. Odată ce expertul a fost finalizat de către un utilizator, nu poate fi lansat din nou de către acesta.

1. Din ecranul Pornire sau Aplicații, efectuați clic pe sau atingeți aplicația **HP Client Security** (Windows 8).

   – sau –

   De pe desktop-ul Windows, efectuați clic pe sau atingeți gadget-ul **HP Client Security** (Windows 7).

   – sau –

   De pe desktop-ul Windows, efectuați dublu clic pe sau atingeți de două ori pictograma **HP Client Security** din zona de notificare, aflată în extrema dreaptă a barei de sarcini.

   – sau –

   De pe desktop-ul Windows, efectuați clic pe sau atingeți pictograma **HP Client Security** din zona de notificare și apoi selectați **Open HP Client Security** (Deschidere HP Client Security).

2. Se va lansa expertul de configurare HP Client Security, care va afișa pagina de întâmpinare.

3. Citiți informațiile prezentate pe pagina de întâmpinare, verificați-vă identitatea tastându-vă parola Windows și apoi efectuați clic pe sau atingeți **Următorul**.

   Dacă nu ați instituit încă o parolă Windows, vi se va solicita să o creați în acest moment. Parola Windows este necesară pentru a vă proteja contul Windows împotriva accesului persoanelor neautorizate și pentru a putea utiliza caracteristicile HP Client Security.

4. Din pagina HP SpareKey, selectați cele 3 întrebări de securitate. Furnizați un răspuns pentru fiecare întrebare și apoi efectuați clic pe **Următorul**. Sunt permise și întrebări personalizate. Pentru mai multe informaţii, consultaţi HP SpareKey—Recuperare parolă, la pagina 14.

5. Din pagina Amprente, înregistraţi cel puţin numărul minim de amprente solicitate şi apoi efectuaţi clic pe sau atingeţi **Următorul**. Pentru mai multe informaţii, consultaţi Amprente, la pagina 12.

6. Din pagina Drive Encryption, activați criptarea, efectuați o copie de rezervă a cheii de criptare și apoi efectuați clic pe sau atingeți **Următorul**. Pentru mai multe informații, consultați secțiunea de Ajutor a software-ului HP Drive Encryption.

NOTĂ: Aceasta se aplică în situațiile în care utilizatorul este administrator, iar expertul de configurare HP Client Security nu a fost configurat anterior de un administrator.

7. Din pagina finală a expertului de configurare, efectuați clic pe sau atingeți **Terminare**.

   Această pagină vă indică starea caracteristicilor și acreditărilor.

8. Expertul de configurare HP Client Security asigură activarea caracteristicilor Just In Time Authentication și File Sanitizer. Pentru mai multe informații, consultați secțiunea de Ajutor a software-ului HP Device Access Manager și a software-ului HP File Sanitizer.

NOTĂ: Aceasta se aplică în situațiile în care utilizatorul este administrator, iar expertul de configurare HP Client Security nu a fost configurat anterior de un administrator.

Deschiderea HP Client Security

Puteți deschide aplicația HP Client Security într-unul din următoarele moduri:

NOTĂ: Expertul de configurare HP Client Security trebuie finalizat înainte de a putea lansa aplicația HP Client Security.

- Din ecranul Pornire sau Aplicații, efectuați clic pe sau atingeți aplicația **HP Client Security**.

  – sau –

  De pe desktop-ul Windows, efectuați clic pe sau atingeți gadget-ul **HP Client Security** (Windows 7).

  – sau –

  De pe desktop-ul Windows, efectuați dublu clic pe sau atingeți de două ori pictograma **HP Client Security** din zona de notificare, aflată în extrema dreaptă a barei de sarcini.

  – sau –

  De pe desktop-ul Windows, efectuați clic pe sau atingeți pictograma **HP Client Security** din zona de notificare și apoi selectați **Open HP Client Security** (Deschidere HP Client Security).

3 Ghid de configurare simplă pentru firme mici

Acest capitol este realizat cu scopul de a explica paşii de bază necesari pentru activarea celor mai frecvente şi utile opţiuni din cadrul HP Client Security pentru firme mici. Numeroasele instrumente şi opţiuni din acest software vă permit să setaţi preferinţele şi să configuraţi controlul de acces. Scopul acestui Ghid de configurare simplă este ca rularea fiecărui modul să fie efectuată cu cel mai mic efort de configurare şi timp. Pentru informaţii suplimentare, selectaţi modulul de care sunteţi interesat şi apoi efectuaţi clic pe **?** sau pe butonul Ajutor din colţul din dreapta sus. Acest buton va afişa automat informaţii care să vă ajute cu fereastra afişată curent.

Noţiuni introductive

1. De pe desktop-ul Windows, deschideţi HP Client Security efectuând dublu clic pe pictograma **HP Client Security** din zona de notificare, aflată în partea dreaptă a barei de activităţi.
2. Introduceţi parola Windows sau creaţi o parolă Windows.
3. Finalizaţi Configurarea HP Client Security.

Pentru a beneficia de HP Client Security este necesar să vă autentificaţi o singură dată în timpul conectării la Windows, consultaţi Caracteristici de securitate, la pagina 27.

Password Manager

Orice persoană deţine un număr ridicat de parole – în special dacă accesaţi în mod regulat site-uri Web sau dacă utilizaţi aplicaţii care necesită să vă conectaţi. Utilizatorul normal fie utilizează aceeaşi parolă pentru fiecare aplicaţie şi site Web, fie devine creativ şi uită rapid care parolă trebuie folosită cu o anumită aplicaţie.

Password Manager poate reţine automat parolele dvs. sau vă oferă posibilitatea să decideţi care site-uri să fie reţinute şi care să fie omise. După ce vă autentificaţi pe computer, Password Manager vă oferă parolele sau acreditările pentru aplicaţiile sau site-uri Web participante.

Atunci când accesaţi orice aplicaţie sau site Web care necesită acreditări, Password Manager va recunoaşte automat site-ul şi va întreba dacă doriţi ca software-ul să reţină informaţiile dvs. Dacă doriţi să excludeţi anumite site-uri, puteţi refuza cererea.

Pentru a începe salvarea locaţiilor Web, numelor de utilizator şi parolelor:

1. Spre exemplu, navigaţi la o aplicaţie sau site Web participante, apoi efectuaţi clic pe pictograma Password Manager în colţul din stânga sus a paginii Web pentru a adăuga autentificarea Web.
2. Denumiţi legătura (opţional) şi introduceţi un nume de utilizator şi o parolă în Password Manager.
3. Când aţi terminat, efectuaţi clic pe butonul **OK**.
4. Password Manager vă poate salva de asemenea numele de utilizator şi parolele pentru partajările de retea sau pentru unităţile de reţea asociate.

Vizualizarea şi gestionarea autentificărilor salvate în Password Manager

Password Manager vă permite să vizualizaţi, să gestionaţi, să efectuaţi o copiere de rezervă şi să lansaţi autentificările dintr-o locaţie centrală. Password Manager acceptă de asemenea lansarea site-urilor salvate din Windows.

Pentru a deschide Password Manager, utilizaţi combinaţia de tastatură Ctrl+tasta Windows+h pentru a deschide Password Manager, apoi efectuaţi clic pe **Conectare** pentru a lansa şi pentru a autentifica scurtătura salvată.

Opţiunea **Editare** din Password Manager vă permite să vizualizaţi şi să modificaţi numele, numele de conectare şi chiar să afişaţi parolele.

HP Client Security pentru firme mici permite copierea de rezervă şi/sau copierea pe un alt computer a tuturor acreditărilor şi setărilor.

HP Device Access Manager

Device Access Manager poate fi utilizat pentru a restricţiona utilizarea diverselor dispozitive de stocare interne şi externe, astfel încât datele dvs. vor rămâne securizate pe unitatea de disc fără a se pierde. Un exemplu ar fi ca atunci când accesul utilizatorului la datele dvs. este permis, să puteţi bloca copierea acestora pe un CD, player de muzică personal sau dispozitiv de memorie USB.

1. Deschideţi **Device Access Manager** (consultaţi Deschiderea Device Access Manager, la pagina 43).

   Se afişează accesul pentru utilizatorul curent.

2. Pentru a modifica accesul pentru utilizatori, grupuri sau dispozitive, efectuaţi clic pe sau atingeţi **Modificare**. Pentru mai multe informaţii, consultaţi Vizualizare sistem, la pagina 44.

HP Drive Encryption

HP Drive Encryption este utilizat pentru a vă proteja datele prin criptarea întregii unităţi de disc. Datele de pe unitatea de disc vor rămâne protejate dacă PC-ul dvs. este furat şi/sau dacă unitatea de disc este scoasă din computerul iniţial şi montată într-un alt computer.

Un avantaj suplimentar de securitate este faptul că Drive Encryption vă solicită să vă autentificaţi corect utilizând numele de utilizator şi parola înainte de pornirea sistemului de operare. Acest proces se numeşte autentificarea prealabilă încărcării.

Pentru a vă uşura munca, mai multe module de software sincronizează automat parolele, inclusiv conturile de utilizator Windows, domeniile de autentificare, HP Drive Encryption, Password Manager şi HP Client Security.

Pentru a configura HP Drive Encryption în timpul configurării iniţiale folosind Expertul de instalare HP Client Security, consultaţi Noţiuni introductive, la pagina 8.

4 HP Client Security

Pagina de întâmpinare HP Client Security este zona centrală care oferă un acces rapid la caracteristicile, aplicațiile și configurările HP Client Security. Pagina de întâmpinare este împărțită în trei secțiuni:

- **DATE**—Oferă acces la aplicațiile folosite pentru gestionarea securității datelor.
- **DISPOZITIV**—Oferă acces la aplicațiile folosite pentru gestionarea securității dispozitivului.
- **IDENTITATE**—Oferă posibilitatea înregistrării și gestionării acreditărilor de autentificare.

Deplasați cursorul deasupra titlului unei aplicații pentru a afișa descrierea aplicației.

HP Client Security poate oferi legături către configurările utilizatorului și cele administrative, aflate în partea de jos a paginii. HP Client Security oferă acces la Configurările avansate, prin atingerea sau executarea unui clic pe pictograma cu (configurări) pentru **Echipament**.

Caracteristici, aplicații și configurări ale identității

Caracteristici, aplicații și configurări ale identității, furnizată de HP Client Security, vă oferă asistență în gestionarea diferitelor aspecte ale identității dvs. digitale. Efectuați clic pe sau atingeți una din următoarele file din pagina de întâmpinare HP Client Security și apoi tastați parola dvs. Windows:

- **Amprente**—Înregistrează și gestionează acreditarea dvs. privind amprenta.
- **SpareKey**—Configurează și gestionează acreditarea dvs. HP SpareKey, care se poate utiliza pentru autentificarea pe computerul dvs., în cazul în care s-au pierdut alte acreditări. De asemenea, vă permite să vă resetați parola uitată.
- **Parolă Windows**—Vă facilitează schimbarea parolei Windows.
- **Dispozitive Bluetooth**—Vă permite să vă înregistrați și să vă gestionați dispozitivele Bluetooth.
- **Carduri**—Vă permite să vă înregistrați și să vă gestionați smart cardurile, cardurile fără contact și cardurile de proximitate.
- **PIN**—Vă permite să vă înregistrați și să vă gestionați acreditarea PIN.
- **RSA SecurID**—Vă permite să înregistraţi şi să vă gestionaţi acreditarea RSA SecurID (dacă s-a realizat instalarea adecvată).
- **Password Manager**—Vă permite să vă gestionați parolele pentru conturile și aplicațiile online.

Amprente

Expertul de configurare HP Client Security vă îndrumă în cadrul procesului de configurare sau „înregistrare” a amprentelor dvs.

De asemenea, puteți să înregistrați sau să vă ștergeți amprentele din pagina Amprente, pe care o puteți accesa efectuând clic sau atingând pictograma **Amprente** din pagina de întâmpinare HP Client Security.

1. Din pagina Amprente, trageți cu degetul până ce aceasta s-a înregistrat cu succes.

   Numărul de degete necesar pentru înregistrare este indicat pe pagină. Sunt preferabile degetul mare sau arătător.

2. Pentru a șterge amprentele înregistrate anterior, efectuați clic pe sau atingeți **Ștergere**.
3. Pentru a înregistra alte degete, efectuați clic pe sau atingeți **Enroll an additional fingerprint** (Înregistrare amprentă suplimentară).
4. Efectuați clic pe sau atingeți **Salvare** înainte de a părăsi pagina.

⚠ **ATENŢIE:** Atunci când înregistrați amprente cu ajutorul expertului, informațiile despre amprente nu se salvează până ce nu ați efectuat clic pe **Următorul**. În cazul în care computerul este inactiv pentru o anumită perioadă de timp sau dacă închideți programul, modificările pe care le-ați efectuat **nu** se salvează.

- Pentru a accesa Configurări administrative pentru amprente, de unde administratorii pot specifica înregistrarea, acuratețea sau alte configurări, efectuați clic pe sau atingeți **Administrative Settings** (Configurări administrative) (necesită privilegii administrative).
- Pentru a accesa Configurările utilizatorului pentru amprente, de unde se pot preciza configurările referitoare la aspectul și comportamentul de recunoaștere a amprentei, efectuați clic pe sau atingeți **Configurări utilizator**.

Configurări administrative pentru amprente

Administratorii pot specifica înregistrarea, acuratețea și alte configurări pentru un cititor de amprente. Sunt necesare privilegii administrative.

- Pentru a accesa Configurări administrative pentru acreditarea amprentei, efectuați clic pe sau atingeți **Administrative Settings** (Configurări administrative) din pagina Amprente.

- **User enrollment** (Înregistrare utilizator)—Alegeți numărul minim și maxim de amprente pe care îl poate înregistra un utilizator.
- **Recunoaștere**—Deplasați cursorul pentru a ajusta sensibilitatea utilizată de cititorul de amprente atunci când trageți cu degetul.

  Dacă amprenta dvs. nu este recunoscută în mod adecvat, va trebui să selectați un nivel de recunoaștere inferior. Un nivel mai înalt de recunoaștere sporește sensibilitatea la variații în momentul tragerii cu degetul pentru identificarea amprentei și, așadar, descrește posibilitatea unei false acceptări. Configurarea **Mediu-înalt** oferă o combinație adecvată între securitate și confort.

Configurările utilizatorului pentru amprente

Din pagina Configurările utilizatorului pentru amprente, puteți specifica configurările care se aplică pentru aspectul și comportamentul sistemului de recunoaștere a amprentelor.

▲ Pentru a accesa Configurările utilizatorului pentru acreditarea amprentei, efectuați clic pe sau atingeți **Configurările utilizatorului** din pagina Amprente.

- **Activare feedback sunet**—În mod predefinit, HP Client Security vă oferă feedback audio în momentul în care s-a trecut cu degetul în vederea amprentării, redând diferite sunete pentru evenimente specifice din cadrul programului. Acum puteți aloca noi sunete acestor evenimente, folosind fila Sunete din configurările de Sunet din panoul de control Windows sau, pentru a dezactiva feedback-ul sonor, debifați caseta de bifare.
- **Show scan quality feedback** (Arată feedback privind calitatea scanării)—Pentru a afișa toate mișcările de tragere cu degetele, indiferent de calitate, selectați caseta de bifare. Pentru a afișa numai gesturile de tragere cu degetul care au o calitate adecvată, debifați caseta de bifare.

HP SpareKey—Recuperare parolă

HP SpareKey vă permite să beneficiați de acces la computerul dvs. (pe platformele compatibile) răspunzând la trei întrebări de securitate.

HP Client Security vă va solicita să vă configurați propria dvs. HP SpareKey pe durata configurării inițiale, din expertul de configurare HP Client Security.

Pentru a vă configura HP SpareKey:

1. Din pagina HP SpareKey a expertului, selectați trei întrebări de securitate și apoi furnizați un răspuns la fiecare întrebare.

   Puteți selecta o întrebare dintr-o listă predefinită sau puteți scrie propria întrebare.

2. Efectuați clic pe sau atingeți **Înregistrare**.

Pentru a vă șterge HP SpareKey:

▲ Efectuați clic pe sau atingeți **Delete your SpareKey** (Ștergere SpareKey).

După configurarea SpareKey, vă puteți accesa computerul folosind SpareKey dintr-un ecran de conectare pentru autentificare la pornire sau din ecranul de întâmpinare Windows.

Puteți selecta diferite întrebări sau vă puteți modifica răspunsurile din pagina SpareKey, care poate fi accesată din fila recuperare parolă din pagina de întâmpinare HP Client Security.

Pentru a accesa configurările HP SpareKey, unde un administrator poate preciza configurările privitoare la acreditarea HP SpareKey, efectuați clic pe **Configurări** (necesită privilegii administrative).

HP SpareKey Settings

Din pagina Configurări HP SpareKey, puteți preciza configurările aplicabile comportamentului și utilizării acreditării HP SpareKey.

▲ Pentru a lansa pagina de configurări HP SpareKey, efectuați clic pe sau atingeți **Configurări** din pagina HP SpareKey (necesită privilegii administrative).

Administratorii pot selecta următoarele configurări:

- Specificați întrebările care îi sunt prezentate fiecărui utilizator pe durata configurării HP SpareKey.
- Adăugați maxim trei întrebări personalizate de siguranță la lista prezentată utilizatorilor.
- Alegeți dacă doriți sau nu să le permiteți utilizatorilor să-și scrie propriile întrebări de securitate.
- Specificați ce medii de autentificare (Windows sau autentificare la pornire) permit utilizarea HP SpareKey pentru recuperarea parolei.

Parolă Windows

HP Client Security simplifică și accelerează schimbarea parolei dvs. Windows. Astfel, procesul este mai rapid decât dacă s-ar fi utilizat panoul de control Windows.

Pentru a vă schimba parola Windows:

1. Din pagina de întâmpinare HP Client Security, efectuați clic pe sau atingeți **Parolă Windows**.
2. Tastați-vă parola actuală în caseta text **Current Windows password** (Parolă Windows curentă).
3. Tastați o nouă parolă în caseta de text **New Windows Password** (Parolă Windows nouă) și apoi tastați-o din nou în caseta de text **Confirmați parola nouă**.
4. Efectuați clic pe sau atingeți **Schimbare** pentru a vă schimba imediat parola actuală cu cea nouă pe care ați tastat-o.

Dispozitive Bluetooth

Dacă administratorul dvs. a activat Bluetooth ca și acreditare de autentificare, puteți configura un telefon Bluetooth alături de alte acreditări, pentru mai multă securitate.

NOTĂ: Sunt acceptate numai telefoane cu Bluetooth.

1. Asigurați-vă că ați activat funcționalitatea Bluetooth pe computer și că telefonul Bluetooth este configurat astfel încât să poată fi descoperit. Pentru a conecta telefonul, poate fi necesar să tastați un cod generat automat pe dispozitivul Bluetooth. În funcție de configurările dispozitivului Bluetooth, poate fi necesară o comparație a codurilor de intrare în legătură între computer și telefon.
2. Pentru a înregistra telefonul, selectați-l și apoi efectuați clic pe sau atingeți **Înregistrare**.

Pentru a accesa Configurări dispozitive Bluetooth, la pagina 15, unde administratorul poate preciza configurările pentru dispozitivele Bluetooth, efectuați clic pe **Configurări** (necesită privilegii administrative).

Configurări dispozitive Bluetooth

Administratorii pot specifica următoarele configurări aplicabile comportamentului și utilizării acreditărilor dispozitivului Bluetooth:

Autentificare silențioasă

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity** (Folosiți automat dispozitivul dvs. Bluetooth înregistrat și conectat, pe durata verificării identității dvs.)—Selectați caseta de bifare pentru a le permite utilizatorilor să folosească acreditarea Bluetooth pentru autentificare, fără a fi necesară vreo acțiune din partea utilizatorului, sau debifați respectiva căsuță pentru a dezactiva această opțiune.

Proximitate Bluetooth

- **Blocaţi computerul atunci când dispozitivul Bluetooth înregistrat iese din aria de acoperire a computerului dvs**—Selectaţi caseta de bifare pentru a bloca computerul atunci când un dispozitiv Bluetooth care a fost conectat pe durata autentificării iese din aria de acoperire sau debifaţi căsuţa pentru a dezactiva această opţiune.

NOTĂ: Modulul Bluetooth de pe computerul dvs. trebuie să aibă această capacitate, pentru a se putea folosi această caracteristică.

Carduri

HP Client Security este compatibil cu mai multe tipuri diferite de carduri de identificare, care sunt niște carduri mici, din plastic, ce includ un cip de computer. Acestea includ smart cardurile, cardurile fără contact și cardurile de proximitate. Dacă unul dintre aceste carduri, precum și cititorul adecvat de carduri, sunt conectate la computer, dacă administratorul a instalat driverul aferent furnizat de producător și dacă administratorul a activat cardul ca și acreditare de autentificare, atunci puteți utiliza cardul pe post de acreditare de autentificare.

Pentru smart carduri, producătorul ar trebui să furnizeze instrumentele necesare instalării unui certificat de securitate și gestionării PIN-ului pe care HP Client Security le utilizează în algoritmul său de securitate. Numărul și tipul de caractere folosite în codul PIN poate varia. Administratorul trebuie să inițializeze smart cardul înainte ca acesta să poată fi folosit.

Următoarele formate de smart card sunt acceptate de HP Client Security:

- CSP
- PKCS11

Următoarele formate de carduri fără contact sunt acceptate de HP Client Security:

- Carduri de memorie fără contact HID iCLASS
- Cardurile de memorie fără contact MiFare Classic 1k, 4 k și mini

Următoarele carduri de proximitate sunt acceptate de HP Client Security:

- Carduri de proximitate HID

Pentru a înregistra un smart card:

1. Introduceți cardul în cititorul de smart card atașat.
2. Atunci când cardul este recunoscut, tastați PIN-ul cardului și apoi efectuați clic pe sau atingeți **Înregistrare**.

Pentru a schimba PIN-ul unui smart card:

1. Introduceți cardul în cititorul de smart card atașat.
2. Atunci când cardul este recunoscut, tastați PIN-ul cardului și apoi efectuați clic pe sau atingeți **Autentificare**.
3. Efectuați clic pe sau atingeți **Modificare PIN** și apoi tastați noul cod PIN.

Pentru a înscrie un card fără contact sau de proximitate:

1. Puneți cardul pe sau foarte aproape de cititorul adecvat.
2. Atunci când cardul este recunoscut, efectuați clic pe sau atingeți **Înregistrare**.

Pentru a șterge un card înregistrat:

1. Puneți cardul în dreptul cititorului.
2. Numai pentru smart carduri: tastați PIN-ul aferent cardului și apoi efectuați clic pe sau atingeți **Autentificare**.
3. Efectuați clic pe sau atingeți **Ștergere**.

Odată ce cardul a fost înregistrat, detaliile privind cardul sunt afișate în secțiunea **Enrolled Cards** (Carduri înregistrate). Atunci când un card a fost șters, va fi eliminat și din listă.

Pentru a accesa configurările cardurilor de proximitate, fără contact și ale smart cardurilor, unde administratorii pot preciza configurările referitoare la acreditările cardului, efectuați clic pe sau atingeți **Configurări** (necesită privilegii administrative).

Configurările cardurilor de proximitate, fără contact și ale smart cardurilor

Pentru a accesa configurările unui card, efectuați clic pe sau atingeți cardul din listă și apoi efectuați clic pe sau atingeți săgeata care se afișează.

Pentru a schimba PIN-ul unui smart card:

1. Puneți cardul în dreptul cititorului.
2. Tastați PIN-ul aferent cardului și apoi efectuați clic pe sau atingeți **Continuare**.
3. Tastați și confirmați noul PIN și apoi efectuați clic pe sau atingeți **Continuare**.

Pentru a inițializa PIN-ul unui smart card:

1. Puneți cardul în dreptul cititorului.
2. Tastați PIN-ul aferent cardului și apoi efectuați clic pe sau atingeți **Continuare**.
3. Tastați și confirmați noul PIN și apoi efectuați clic pe sau atingeți **Continuare**.
4. Efectuați clic pe sau atingeți **Da** pentru a confirma inițializarea.

Pentru a șterge datele cardului:

1. Puneți cardul în dreptul cititorului.
2. Tastați PIN-ul aferent cardului (numai pentru smart carduri) și apoi efectuați clic pe sau atingeți **Continuare**.
3. Efectuați clic pe sau atingeți **Da** pentru a confirma ștergerea.

PIN

Dacă administratorul dvs. a activat un cod PIN ca și acreditare de autentificare, puteți configura un cod PIN alături de alte acreditări, pentru mai multă securitate.

Pentru a configura un nou PIN:

▲ Tastați PIN-ul, apoi tastați-l din nou pentru confirmare și efectuați clic pe sau atingeți **Aplicare**.

Pentru a șterge un cod PIN:

▲ Efectuați clic pe sau atingeți **Ștergere** și apoi efectuați clic pe sau atingeți **Da** pentru a confirma.

Pentru a accesa configurările PIN, de unde administratorii pot preciza configurările referitoare la acreditările PIN, efectuați clic pe sau atingeți **Configurări** (necesită privilegii administrative).

Setări PIN

Din pagina Configurări PIN, puteți specifica lungimea minimă și maximă acceptabilă a acreditării PIN.

RSA SecurID

Dacă administratorul a activat RSA ca și acreditare de autentificare, iar următoarele condiții sunt adevărate, atunci puteți înregistra sau șterge o acreditare RSA SecurID.

NOTĂ: Este necesară o configurare adecvată.

- Este necesar ca utilizatorul să fi fost creat pe un server RSA.
- Tokenul RSA SecurID alocat utilizatorului și computerului trebuie să fi fost asociat domeniului serverului RSA.
- Software-ul SecurID este instalat pe computer.
- Este disponibilă o conexiune la serverul RSA configurat adecvat.

Pentru a înregistra o acreditare RSA SecurID:

▲ Tastați numele de utilizator și parola RSA SecurID (codul tokenului RSA SecurID sau PIN + codul tokenului, în funcție de mediu) și apoi efectuați clic pe sau atingeți **Aplicare**.

Dacă înregistrarea reușește, se afișează un mesaj „Acreditarea dvs. RSA SecurID a fost înregistrată cu succes”, iar butonul Ștergere este activat.

Pentru a șterge o acreditare RSA SecurID:

▲ Efectuați clic pe **Ștergere** și apoi selectați **Da** pentru dialogul popup care întreabă „Sunteți sigur că doriți să ștergeți acreditarea RSA SecurID?”

Password Manager

Autentificarea pe site-urile web și în cadrul aplicațiilor este acum mai ușoară și mai sigură, cu ajutorul Password Manager. Puteți crea parole mai puternice care nu trebuie scrise sau memorate, și apoi vă puteți autentifica rapid și ușor cu ajutorul unei amprente, smart card, card de proximitate, card fără contact, telefon Bluetooth, cod PIN, acreditare RSA sau cu ajutorul parolei dvs. Windows.

NOTĂ: Din cauza structurii în continuă schimbare a ecranelor de conectare web, este posibil ca Password Manager să nu fie întotdeauna compatibil cu orice site web.

Password Manager oferă următoarele opțiuni:

Pagina Password Manager

- Efectuați clic pe sau atingeți un cont pentru a lansa automat o pagină web sau o aplicație și pentru a vă autentifica.
- Folosiți categoriile pentru a vă organiza conturile.

Nivelul parolei

- Puteți observa imediat dacă una dintre parolele dvs. prezintă un risc de securitate.
- Atunci când adăugați datele de conectare, verificați nivelul parolelor individuale folosite pentru site-uri web și aplicații.
- Nivelul parolei este ilustrat de indicatori de stare, de culoare roșie, galbenă sau verde.

Pictograma **Password Manager** este afișată în colțul din stânga sus al unei pagini web sau al ecranului de conectare al aplicației. Atunci când nu s-au creat date de conectare pentru respectivul site web sau pentru respectiva aplicație, pe pictogramă se va afișa un semn în formă de plus.

▲ Efectuați clic pe sau atingeți pictograma **Password Manager** pentru a afișa un meniu contextual, unde veți putea alege dintre următoarele opțiuni:

- Adăugare [somedomain.com] la Password Manager
- Deschidere Password Manager
- Configurări pictogramă
- Ajutor

În cazul paginilor web sau programelor pentru care nu s-au creat încă date de conectare

Următoarele opțiuni sunt afișate în meniul contextual:

- **Add [somedomain.com] to the Password Manager** (Adăugare [somedomain.com] la Password Manager)—Vă permite să adăugați date de conectare la ecranul actual de conectare.
- **Open Password Manager** (Deschidere Password Manager)—Lansează Password Manager.
- **Configurări pictograme**—Vă permite să specificați condițiile în care se afișează pictograma **Password Manager**.
- **Ajutor**—Afișează secțiunea Ajutor a HP Client Security.

În cazul paginilor web sau programelor pentru care s-au creat deja date de conectare

Următoarele opțiuni sunt afișate în meniul contextual:

- **Fill in logon data** (Completare date de conectare)—Afișează pagina **Verify your identity** (Verificați-vă identitatea). Dacă v-ați autentificat cu succes, datele dvs. de conectare sunt plasate în câmpurile de conectare, iar pagina este transmisă (dacă transmiterea a fost specificată atunci când datele de conectare au fost create sau modificate ultima oară).
- **Edit Logon** (Modificare date de conectare)—Vă permite să vă modificați datele de conectare pentru acest site web.
- **Add Logon** (Adăugare date de conectare)—Vă permite să adăugați un cont la Password Manager.
- **Open Password Manager** (Deschidere Password Manager)—Lansează Password Manager.
- **Ajutor**—Afișează secțiunea Ajutor a HP Client Security.

NOTĂ: Este posibil ca administratorul acestui computer să fi configurat HP Client Security pentru a solicita mai mult de o singură acreditare atunci când se verifică identitatea dvs.

Adăugare date de conectare

Puteți adăuga cu ușurință date de conectare pentru un site web sau un program, tastând o singură dată informațiile de conectare. Din acel moment, Password Manager va completa automat informațiile, în locul dvs. Puteți folosi aceste date de conectare după ce ați răsfoit site-ul web sau în interiorul programului.

Pentru a adăuga date de conectare:

1. Deschideți ecranul de conectare al unui site web sau program.
2. Efectuați clic pe sau atingeți pictograma **Password Manager** și apoi efectuați clic pe sau atingeți una dintre următoarele opțiuni, în funcție de faptul dacă ecranul de conectare este pentru un site web sau un program:
   - Pentru un site web, efectuați clic pe sau atingeți **Add [domain name] to Password Manager** (Adăugați [domain name] la Password Manager).
   - Pentru un program, efectuați clic pe sau atingeți **Add this logon screen to Password Manager** (Adăugați acest ecran de conectare la Password Manager).
3. Tastați-vă datele de conectare. Câmpurile de conectare de pe ecran, precum și câmpurile corespunzătoare din caseta de dialog, sunt marcate cu un chenar portocaliu îngroșat.
   a. Pentru a completa un câmp de conectare cu una dintre opțiunile pre-formatate, efectuați clic pe sau atingeți săgețile din partea dreaptă a câmpului.
   b. Pentru a vizualiza parola pentru aceste date de conectare, efectuați clic pe sau atingeți **Afișare parolă**.
   c. Pentru ca aceste câmpuri de conectare să se completeze, fără însă a se și trimite, debifați caseta **Automatically submit logon data** (Transmitere automată date de conectare).
   d. Efectuați clic pe sau atingeți **OK** pentru a selecta metoda de autentificare pe care doriți să o utilizați (amprente, smart card, card de proximitate, card fără contact, telefon Bluetooth, PIN sau parolă) și apoi conectați-vă folosind metoda de autentificare selectată.

      Semnul plus va dispărea de pe pictograma **Password Manager**, înștiințându-vă astfel că datele de conectare au fost create.
   e. Dacă Password Manager nu detectează câmpurile de conectare, efectuați clic pe sau atingeți **More fields** (Mai multe câmpuri).
      - Selectați caseta de bifare pentru fiecare câmp necesar pentru conectare sau deselectați-o pentru orice câmpuri care nu sunt necesare în scopuri de conectare.
      - Efectuați clic pe sau atingeți **Închidere**.

De fiecare dată când accesați respectivul site web sau deschideți programul respectiv, pictograma **Password Manager** este afișată în colțul din stânga sus al ecranului de conectare al site-ului sau aplicației, fapt care arată că puteți să vă utilizați acreditările înregistrate pentru a vă conecta.

Modificare date de conectare

Pentru a modifica datele de conectare:

1. Deschideți ecranul de conectare al unui site web sau program.
2. Pentru a afișa caseta de dialog în care vă puteți modifica informațiile de conectare, efectuați clic pe sau atingeți pictograma **Password Manager** și apoi efectuați clic pe sau atingeți **Edit Logon** (Modificare date de conectare).

   Câmpurile de conectare de pe ecran, precum și câmpurile corespunzătoare din caseta de dialog, sunt marcate cu un chenar portocaliu îngroșat.

   De asemenea, puteți modifica informațiile privind contul din pagina Password Manager, efectuând clic pe sau atingând datele de conectare în vederea afișării opțiunilor de modificare și apoi selectând **Modificare**.

3. Modificați-vă informațiile de conectare.

   - Pentru a modifica secțiunea **Nume cont**, tastați un nou nume în câmp.
   - Pentru a adăuga sau a modifica un nume de **Categorie**, tastați sau modificați numele din câmpul **Categorie**.
   - Pentru a selecta un câmp de conectare **Nume de utilizator** cu una dintre opțiunile pre-formatate, efectuați clic pe sau atingeți săgețile din partea dreaptă a câmpului.

     Opțiunile pre-formatate sunt disponibile numai atunci când se modifică datele de conectare cu ajutorul comenzii Modificare, din meniul contextual aferent pictogramei Password Manager.
   - Pentru a selecta un câmp de conectare **Parolă** cu una dintre opțiunile pre-formatate, efectuați clic pe sau atingeți săgețile din partea dreaptă a câmpului.

     Opțiunile pre-formatate sunt disponibile numai atunci când se modifică datele de conectare cu ajutorul comenzii Modificare, din meniul contextual aferent pictogramei Password Manager.
   - Pentru a adăuga câmpuri suplimentare din ecran la datele dvs. de conectare, efectuați clic pe sau atingeți **More fields** (Mai multe câmpuri).
   - Pentru a vizualiza parola pentru aceste date de conectare, efectuați clic pe sau atingeți pictograma **Afișare parolă**.
   - Pentru ca aceste câmpuri de conectare să se completeze, fără însă a se și trimite, debifați caseta **Automatically submit logon data** (Transmitere automată date de conectare).
   - Pentru a marca aceste date de conectare ca având o parolă compromisă, selectați caseta de bifare **This password is compromised** (Această parolă este compromisă).

     După ce modificările au fost salvate, orice alte date de conectare ce partajează aceeași parolă vor fi de asemenea marcate ca fiind compromise. Puteți apoi să vizitați fiecare cont afectat și puteți schimba parolele după cum va fi necesar.

4. Efectuați clic pe sau atingeți **OK**.

Folosind meniul Legături rapide din Password Manager

Password Manager vă oferă o modalitate rapidă și ușoară pentru a lansa site-uri web și programe pentru care ați creat date de conectare. Efectuați dublu clic pe sau atingeți de două ori datele de conectare pentru un program sau un site web din meniul **Password Manager Quick Links** (Legături rapide Password Manager) sau din pagina Password Manager a HP Client Security, pentru a deschide ecranul de conectare și apoi completați-vă datele de conectare.

Atunci când creați date de conectare, acestea sunt adăugate automat la meniul dvs. **Legături rapide** din Password Manager.

Pentru a afișa meniul **Legături rapide**:

▲ Apăsaţi combinaţia de comenzi rapide **Password Manager** (Ctrl+tasta Windows+h este setarea din fabrică). Pentru a schimba combinația de comenzi rapide, din pagina de întâmpinare HP Client Security, efectuați clic pe **Password Manager** și apoi efectuați clic pe sau atingeți **Configurări**.

Organizarea datelor de conectare pe categorii

Creați una sau mai multe categorii pentru a vă menține în ordine datele de conectare.

Pentru a aloca anumite date de conectare unei categorii:

1. Din pagina de întâmpinare HP Client Security, efectuați clic pe sau atingeți **Password Manager**.
2. Efectuați clic pe sau atingeți un cont și apoi efectuați clic pe sau atingeți **Modificare**.
3. În câmpul **Categorie** tastați un nume pentru categorie.
4. Efectuați clic pe sau atingeți **Salvare**.

Pentru a șterge un cont dintr-o categorie:

1. Din pagina de întâmpinare HP Client Security, efectuați clic pe sau atingeți **Password Manager**.
2. Efectuați clic pe sau atingeți un cont și apoi efectuați clic pe sau atingeți **Modificare**.
3. Din câmpul **Categorie** ștergeți denumirea categoriei.
4. Efectuați clic pe sau atingeți **Salvare**.

Pentru a redenumi o categorie:

1. Din pagina de întâmpinare HP Client Security, efectuați clic pe sau atingeți **Password Manager**.
2. Efectuați clic pe sau atingeți un cont și apoi efectuați clic pe sau atingeți **Modificare**.
3. Din câmpul **Categorie** modificați denumirea categoriei.
4. Efectuați clic pe sau atingeți **Salvare**.

Gestionarea datelor de conectare

Cu ajutorul Password Manager, toate informațiile de conectare - nume de utilizatori, parole și conturi cu conectare multiplă - sunt gestionate dintr-un singur loc central.

Datele dvs. de conectare sunt indicate în pagina Password Manager.

Pentru a vă gestiona datele de conectare:

1. Din pagina de întâmpinare HP Client Security, efectuați clic pe sau atingeți **Password Manager**.
2. Efectuați clic pe sau atingeți date de conectare existente și apoi selectați una dintre următoarele opțiuni, urmând instrucțiunile de pe ecran:
   - **Modificare**—Modifică datele de conectare. Pentru mai multe informaţii, consultaţi Modificare date de conectare, la pagina 20.
   - **Autentificare**—Pentru autentificarea în contul selectat.
   - **Ștergere**—Șterge datele de conectare pentru contul selectat.

Pentru a adăuga date suplimentare de conectare, pentru un site web sau program:

1. Deschideți ecranul de conectare al unui site web sau program.
2. Efectuați clic pe sau atingeți pictograma **Password Manager** pentru a-i afișa meniul contextual.
3. Efectuați clic pe sau atingeți **Add Logon** (Adăugare date de conectare) și apoi urmaţi instrucţiunile de pe ecran.

Evaluarea nivelului parolei

Folosirea unor parole cu nivel de securitate înalt în vederea conectării la programele și site-urile dvs. web reprezintă un aspect important al protejării identității dvs.

Password Manager vă facilitează monitorizarea și îmbunătățirea securității, cu ajutorul unei analize instantanee și automate a nivelului fiecăreia dintre parolele folosite pentru conectarea la programele și site-urile dvs. web.

În momentul în care tastați parola pe durata creării datelor de conectare Password Manager pentru un cont, sub parolă se afișează o bară colorată, care indică nivelul de securitate al parolei dvs. Culoarea indică următoarele valori:

- **Roșu**—Nivel de securitate scăzut
- **Galben**—Nivel de securitate mediu
- **Verde**—Nivel de securitate înalt

Configurările pictogramei Password Manager

Password Manager încearcă să identifice ecranele de conectare pentru site-uri web și programe. Atunci când detectează un ecran de conectare pentru care nu ați creat date de conectare, Password Manager vă va solicita să adăugați date de conectare pentru ecranul respectiv, prin afișarea pictogramei **Password Manager** însoțită de semnul plus.

1. Efectuați clic pe sau atingeți pictograma și apoi efectuați clic pe sau atingeți **Icon Settings** (Configurări pictograme) pentru a personaliza modul în care Password Manager gestionează posibilele site-uri de conectare.
   - **Prompt to add logons for logon screens** (Solicită adăugarea de informații de conectare pentru ecranele de conectare)—Efectuați clic pe sau atingeți această opțiune dacă doriți ca Password Manager să vă solicite să adăugați date de conectare atunci când se afișează un ecran de conectare pentru care nu s-au instituit deja informații de conectare.
   - **Exclude this screen** (Exclude acest ecran)—Selectați această casetă de bifare dacă doriți ca Password Manager să nu vă mai solicite să adăugați date de conectare pentru acest ecran de conectare.
   - **Do not prompt to add logons for logon screens** (Nu solicita adăugarea de informații de conectare pentru ecranele de conectare)—Selectați butonul radio.
2. Pentru a adăuga date de conectare la un ecran care a fost exclus anterior:
   a. Conectați-vă la site-ul web exclus anterior.
   b. Pentru ca Password Manager să îşi reamintească parola pentru acest site, efectuaţi clic pe sau atingeţi **Memorare** din dialogul popup pentru a salva parola şi a crea date de conectare pentru respectivul ecran.
3. Pentru a accesa configurările suplimentare Password Manager, efectuați clic pe sau atingeți pictograma Password Manager, efectuați clic pe sau atingeți **Deschidere Password Manager** și apoi efectuați clic pe sau atingeți **Configurări** din pagina Password Manager.

Importare și exportare date de conectare

Din pagina Importare și exportare a HP Password Manager, puteți importa datele de conectare salvate de browserele web pe computerul dvs. De asemenea, puteți importa date dintr-un fișier copie de rezervă HP Client Security și puteți exporta date către un fișier copie de rezervă HP Client Security.

▲ Pentru a lansa pagina Importare și exportare, efectuați clic pe sau atingeți **Import and export** (Importare și exportare) din pagina Password Manager.

Pentru a importa parole dintr-un browser:

1. Efectuați clic pe sau atingeți browserul din care doriți să importați parolele (sunt afișate numai browserele instalate).
2. Debifați caseta aferentă conturilor pentru care nu doriți să importați parole.
3. Efectuaţi clic pe sau atingeţi **Import**.

Importarea datelor din, respectiv exportarea datelor către un fișier copie de rezervă HP Client Security se poate realiza prin legăturile asociate (din **Alte opțiuni**), din pagina Importare și exportare.

NOTĂ: Această caracteristică importă și exportă numai datele Password Manager. Pentru informații despre copierea de rezervă și restaurarea datelor suplimentare HP Client Security, consultați Efectuarea de copii de rezervă și restaurarea datelor dvs, la pagina 28.

Pentru a importa datele dintr-un fișier copie de rezervă HP Client Security:

1. Din pagina Importare și exportare a HP Password Manager, efectuați clic pe sau atingeți **Import data from an HP Client Security backup file** (Importare date dintr-un fișier copie de rezervă HP Client Security).
2. Verificarea identității dvs.
3. Selectați fișierul copie de rezervă creat anterior sau tastați calea în câmpul furnizat și apoi efectuați clic pe sau atingeți **Răsfoire**.
4. Tastați parola folosită pentru protejarea fișierului și apoi efectuați clic pe sau atingeți **Următorul**.
5. Efectuați clic pe sau atingeți **Restaurare**.

Pentru a exporta date într-un fișier copie de rezervă HP Client Security:

1. Din pagina Importare și exportare a HP Password Manager, efectuați clic pe sau atingeți **Export data from an HP Client Security backup file** (Exportare date dintr-un fișier copie de rezervă HP Client Security).
2. Verificați-vă identitatea și apoi efectuați clic pe sau atingeți **Următorul**.
3. Tastați o denumire pentru fișierul copie de rezervă. În mod implicit, fișierul este salvat în folderul dvs. Documente. Pentru a specifica un loc diferit, efectuați clic pe sau atingeți **Răsfoire**.
4. Tastați și confirmați parola folosită pentru protejarea fișierului și apoi efectuați clic pe sau atingeți **Salvare**.

Setări

Puteți preciza configurările pentru personalizarea Password Manager:

- **Prompt to add logons for logon screens** (Solicitare pentru adăugarea de date de conectare la ecranele de conectare)—Pictograma **Password Manager** însoțită de semnul plus este afișată în momentul în care se detectează un ecran de conectare la un site web sau program, fapt care arată că puteți adăuga date de conectare pentru acest ecran la meniul **Logons** (Date de conectare).

  Pentru a dezactiva această caracteristică, debifați caseta de lângă **Prompt to add logons for logon screens** (Solicitare pentru adăugarea de date de conectare la ecranele de conectare).

- **Deschideţi Password Manager cu Ctrl+Win+h**— Comanda rapidă implicită care deschide meniul **Legături rapide Password Manager** este Ctrl+tasta Windows+h.

  Pentru a schimba comanda rapidă, efectuați clic pe sau atingeți această opțiune și apoi tastați o nouă combinaţie de taste. Combinațiile pot include una sau mai multe dintre următoarele taste: ctrl, alt sau shift şi orice taste alfabetice sau numerice.

  Nu se pot folosi combinațiile rezervate pentru Windows sau pentru aplicațiile Windows.

- Pentru a readuce configurările la valorile implicite din fabrică, efectuați clic pe sau atingeți **Restabilire valori implicite**.

Configurări avansate

Administratorii pot accesa următoarele opțiuni selectând pictograma **Echipament** (configurări) din pagina de întâmpinare HP Client Security.

- **Administrator Policies** (Politici de administrator)—Vă permite să configurați politicile de conectare și de sesiune pentru administratori.
- **Standard User Policies** (Politici pentru utilizatorii standard)—Vă permite să configurați politicile de conectare și de sesiune pentru utilizatorii standard.
- **Security Features** (Caracteristici de securitate)—Vă permite să îmbunătățiți securitatea computerului dvs. prin protejarea contului dvs. Windows cu ajutorul unei autentificări puternice și/sau prin activarea autentificării înainte de pornirea sistemului Windows.
- **Utilizatori**—Vă permite să gestionaţi utilizatorii şi acreditările lor.
- **Politicile mele**—Vă permite să vă revizuiți politicile de autentificare și starea înregistrării.
- **Copiere de rezervă și restaurare**—Vă permite să efectuați copii de rezervă sau să vă restaurați datele HP Client Security.
- **Despre HP Client Security**—Afişează informaţii privind versiunea HP Client Security Manager.

Politici de administrator

Puteți configura politicile de conectare și de sesiune pentru administratori, de pe acest computer. Politicile de conectare configurate aici se aplică acreditărilor necesare pentru ca un administrator local să se conecteze la Windows. Politicile de sesiune configurate aici se aplică acreditărilor necesare pentru ca un administrator local să verifice identitatea în cadrul unei sesiuni Windows.

În mod predefinit, toate politicile noi sau schimbate sunt aplicate imediat după ce ați efectuat clic pe sau ați atins **Aplicare**.

Pentru a adăuga o nouă politică:

1. Din pagina de întâmpinare HP Client Security, efectuați clic pe sau atingeți pictograma **Echipament**.
2. Din pagina Setări avansate, efectuaţi clic pe sau atingeţi **Politici de administrator**.
3. Efectuați clic pe sau atingeți **Add new policy** (Adăugare politică nouă).
4. Efectuați clic pe săgețile jos pentru a selecta acreditările primare și (opțional) secundare pentru noua politică și apoi efectuați clic pe sau atingeți **Adăugare**.
5. Efectuaţi clic pe **Aplicare**.

Pentru a întârzia aplicarea unei politici noi sau schimbate:

1. Efectuați clic pe sau atingeți **Enforce this policy immediately** (Aplică imediat această politică).
2. Selectați **Enforce this policy on the specific date** (Aplică această politică la data specificată).
3. Tastați o dată sau utilizați calendarul popup pentru a selecta o dată la care această politică ar trebui aplicată.
4. Dacă doriți, selectați momentul în care utilizatorilor trebuie să li se reamintească noua politică.
5. Efectuaţi clic pe **Aplicare**.

Politici pentru utilizatorii standard

Puteți configura politicile de conectare și de sesiune pentru utilizatorii standard ai acestui computer. Politicile de conectare configurate aici se aplică acreditărilor necesare pentru ca un utilizator standard să se conecteze la Windows. Politicile de sesiune configurate aici se aplică acreditărilor necesare pentru ca un utilizator standard să verifice identitatea în cadrul unei sesiuni Windows.

În mod predefinit, toate politicile noi sau schimbate sunt aplicate imediat după ce ați efectuat clic pe sau ați atins **Aplicare**.

Pentru a adăuga o nouă politică:

1. Din pagina de întâmpinare HP Client Security, efectuați clic pe sau atingeți pictograma **Echipament**.
2. Din pagina Configurări avansate, efectuați clic pe sau atingeți **Standard User Policies** (Politici pentru utilizatorii standard).
3. Efectuați clic pe sau atingeți **Add new policy** (Adăugare politică nouă).
4. Efectuați clic pe săgețile jos pentru a selecta acreditările primare și (opțional) secundare pentru noua politică și apoi efectuați clic pe sau atingeți **Adăugare**.
5. Efectuaţi clic pe **Aplicare**.

Pentru a întârzia aplicarea unei politici noi sau schimbate:

1. Efectuați clic pe sau atingeți **Enforce this policy immediately** (Aplică imediat această politică).
2. Selectați **Enforce this policy on the specific date** (Aplică această politică la data specificată).
3. Tastați o dată sau utilizați calendarul popup pentru a selecta o dată la care această politică ar trebui aplicată.
4. Dacă doriți, selectați momentul în care utilizatorilor trebuie să li se reamintească noua politică.
5. Efectuaţi clic pe **Aplicare**.

Caracteristici de securitate

Puteți activa caracteristicile HP Client Security care vă ajută să vă protejați împotriva accesului neautorizat la computer.

Pentru a configura caracteristicile de securitate:

1. Din pagina de întâmpinare HP Client Security, efectuați clic pe sau atingeți pictograma **Echipament**.
2. Din pagina Configurări avansate, efectuați clic pe sau atingeți **Security Features** (Caracteristici de securitate).
3. Activați caracteristicile de securitate selectând casetele de bifare și apoi efectuați clic pe sau atingeți **Aplicare**. Cu cât selectați mai multe caracteristici, cu atât mai sigur va fi computerul dvs.

   Aceste configurări se aplică tuturor utilizatorilor.

   - **Windows Logon Security** (Securitatea conectării la Windows)—Vă protejează conturile Windows prin aceea că solicită utilizarea acreditărilor HP Client Security în vederea asigurării accesului.
   - **Securitate la preîncărcare (autentificare la pornire)**—Vă protejează computerul înainte ca Windows să pornească. Această selecție nu este disponibilă dacă nu este prevăzută în BIOS.
   - **Allow One Step logon** (Permite conectarea într-o singură etapă)—Această configurare permite eludarea conectării la Windows dacă autentificarea s-a realizat anterior la pornire sau la nivelul Drive Encryption.
4. Efectuaţi clic pe sau atingeţi **Utilizatori** şi apoi efectuaţi clic pe sau atingeţi fila utilizatorului.

Utilizatori

Puteți monitoriza și gestiona utilizatorii HP Client Security de pe acest computer.

Pentru a adăuga un alt utilizator Windows la HP Client Security:

1. Din pagina de întâmpinare HP Client Security, efectuați clic pe sau atingeți pictograma **Echipament**.
2. Din pagina Configurări avansate, efectuați clic pe sau atingeți **Utilizatori**.
3. Efectuați clic pe sau atingeți **Add another Windows user to HP Client Security** (Adăugați un alt utilizator Windows la HP Client Security).
4. Tastați numele utilizatorului pe care doriți să-l adăugați și apoi efectuați clic pe sau atingeți **OK**.
5. Tastați parola de Windows a utilizatorului.

   În pagina Utilizator se va afișa o filă pentru utilizatorul adăugat.

Pentru a șterge un utilizator Windows din HP Client Security:

1. Din pagina de întâmpinare HP Client Security, efectuați clic pe sau atingeți pictograma **Echipament**.
2. Din pagina Configurări avansate, efectuați clic pe sau atingeți **Utilizatori**.
3. Efectuați clic pe sau atingeți numele utilizatorului pe care doriți să-l ștergeți.
4. Efectuaţi clic pe sau atingeţi **Ştergere utilizator** şi apoi efectuaţi clic pe sau atingeţi **Da** pentru a confirma.

Pentru a afișa un rezumat al politicilor de conectare și de sesiune aplicate pentru un utilizator:

▲ Efectuaţi clic pe sau atingeţi **Utilizatori** şi apoi efectuaţi clic pe sau atingeţi fila utilizatorului.

Politicile mele

Puteți să vă afișați politicile de autentificare și starea înregistrării. Pagina Politicile mele oferă de asemenea legături către paginile Politici de administrator și Politici pentru utilizatorii standard.

1. Din pagina de întâmpinare HP Client Security, efectuați clic pe sau atingeți pictograma **Echipament**.
2. Din pagina Configurări avansate, efectuați clic pe sau atingeți **My Policies** (Politicile mele).

   Se afișează politicile de conectare și de sesiune aplicate pentru utilizatorul conectat la momentul respectiv.

Pagina Politicile mele oferă de asemenea legături către Politici de administrator, la pagina 25 și Politici pentru utilizatorii standard, la pagina 26.

Efectuarea de copii de rezervă și restaurarea datelor dvs

Se recomandă să efectuați în mod regulat copii de rezervă ale datelor dvs. HP Client Security. Frecvența cu care realizați aceste copii de rezervă depinde de cât de des se modifică datele. De exemplu, dacă adăugați noi date de conectare în fiecare zi, ar trebui să efectuați în fiecare zi copii de rezervă ale datelor dvs.

Copiile de rezervă pot fi de asemenea utilizate pentru a migra de pe un computer pe altul, fapt cunoscut și sub denumirea de importare și exportare.

NOTĂ: Numai Password Manager beneficiază de o copie de rezervă din partea acestei caracteristici. Drive Encryption are o metodă independentă de realizare a copiilor de rezervă. Informațiile Device Access Manager și cele privind autentificarea prin amprentă nu beneficiază de copii de rezervă.

HP Client Security trebuie instalat pe orice computer care va primi datele tip copie de rezervă, înainte ca datele să poată fi restaurate din fișierul copie de rezervă.

Pentru a efectua copii de rezervă ale datelor dvs.:

1. Din pagina de întâmpinare HP Client Security, efectuați clic pe sau atingeți pictograma **Echipament**.
2. Din pagina Setări avansate, efectuaţi clic pe sau atingeţi **Politici de administrator**.
3. Efectuați clic pe sau atingeți **Copiere de rezervă și restaurare**.
4. Efectuați clic pe sau atingeți **Copiere de rezervă** și apoi verificați-vă identitatea.
5. Selectați modulul pe care doriți să-l includeți în copia de rezervă și apoi efectuați clic pe sau atingeți **Următorul**.
6. Tastați o denumire pentru fișierul de stocare. În mod implicit, fișierul este salvat în folderul dvs. Documente. Pentru a specifica un loc diferit, efectuați clic pe sau atingeți **Răsfoire**.
7. Tastați și confirmați o parolă pentru a proteja fișierul.
8. Efectuați clic pe sau atingeți **Salvare**.

Pentru a vă restaura datele:

1. Din pagina de întâmpinare HP Client Security, efectuați clic pe sau atingeți pictograma **Echipament**.
2. Din pagina Setări avansate, efectuaţi clic pe sau atingeţi **Politici de administrator**.
3. Efectuați clic pe sau atingeți **Copiere de rezervă și restaurare**.
4. Selectați **Restaurare** și apoi verificați-vă identitatea.
5. Selectați fișierul de stocare creat anterior. Tastați calea în câmpul furnizat. Pentru a specifica un loc diferit, efectuați clic pe sau atingeți **Răsfoire**.
6. Tastați parola folosită pentru protejarea fișierului și apoi efectuați clic pe sau atingeți **Următorul**.
7. Selectați modulele pentru care doriți să restaurați datele.
8. Efectuați clic pe sau atingeți **Restaurare**.

5 HP Drive Encryption (numai la anumite modele)

HP Drive Encryption oferă o protecție completă a datelor, prin criptarea datelor de pe computerul dvs. Atunci când Drive Encryption este activat, trebuie să vă conectaţi din ecranul de conectare Drive Encryption, afişat înainte de pornirea sistemului de operare Windows ®.

Ecranul de întâmpinare HP Client Security le permite administratorilor Windows să activeze Drive Encryption, să efectueze copii de rezervă ale cheii de criptare și să selecteze sau să deselecteze unitățile sau partițiile în vederea criptării. Pentru mai multe informații, consultați secțiunea de Ajutor a software-ului HP Client Security.

Următoarele sarcini pot fi realizate cu ajutorul Drive Encryption:

- Selectarea configurărilor Drive Encryption:
  - Criptarea sau decriptarea unităților sau partițiilor individuale folosind criptarea software
  - Criptarea sau decriptarea unităților individuale cu criptare automată folosind criptarea hardware
  - Adăugarea unei securități suplimentare prin dezactivarea modurilor Repaus sau În așteptare, pentru a vă asigura că autentificarea Drive Encryption, prealabilă pornirii, este întotdeauna solicitată

NOTĂ: Numai unitatea de disc internă SATA și cea externă eSATA pot fi criptate.

- Crearea cheilor de rezervă
- Recuperarea accesului la un computer criptat folosind chei de rezervă și HP SpareKey
- Activarea autentificării Drive Encryption, prealabile pornirii, folosindu-se o parolă, o amprentă înregistrată sau un PIN pentru smart cardurile selectate

Deschiderea Drive Encryption

Administratorii pot accesa Drive Encryption prin deschiderea HP Client Security:

1. Din ecranul Pornire, efectuați clic pe sau atingeți aplicația **HP Client Security** (Windows 8).

   – sau –

   De pe desktop-ul Windows, efectuați dublu clic pe sau atingeți de două ori pictograma **HP Client Security** din zona de notificare, aflată în extrema dreaptă a barei de sarcini.

2. Efectuați clic pe sau atingeți pictograma **Drive Encryption**.

Activităţi generale

Activarea Drive Encryption pentru unitățile de disc standard.

Unitățile de disc standard sunt criptate folosindu-se criptarea software. Urmați acești pași pentru a cripta o unitate sau o partiție de disc:

1. Lansați **Drive Encryption**. Pentru mai multe informaţii, consultaţi Deschiderea Drive Encryption, la pagina 30.
2. Selectați caseta de bifare pentru unitatea sau partiția pe care doriți să o criptați și apoi efectuați clic pe sau atingeți **Cheie de rezervă**.

NOTĂ: Pentru o mai bună securitate, selectați caseta de bifare **Disable sleep mode for increased security** (Dezactivare mod repaus pentru o securitate sporită). Atunci când dezactivați modul repaus, nu există niciun risc ca acreditările folosite pentru deblocarea unității să fie stocate în memorie.

3. Selectați una sau mai multe dintre opțiunile de copiere de rezervă și apoi efectuați clic pe sau atingeți **Copiere de rezervă**. Pentru mai multe informaţii, consultaţi Copierea de rezervă a cheilor de criptare, la pagina 34.
4. Puteți continua să lucrați în timp ce se execută copierea de rezervă a cheii de criptare. Nu reporniți computerul.

NOTĂ: Vi se va solicita să reporniți computerul. După repornire, se afișează ecranul de preîncărcare Drive Encryption, care va solicita datele de autentificare înainte ca sistemul Windows să pornească.

Drive Encryption a fost activat. Criptarea partiției/partițiilor unității selectate poate dura mai multe ore, în funcție de numărul și dimensiunea partiției/partițiilor.

Pentru mai multe informații, consultați secțiunea de Ajutor a software-ului HP Client Security.

Activarea Drive Encryption pentru unitățile cu criptare automată

Unitățile cu criptare automată care respectă specificația OPAL a Trusted Computing Group pentru gestionarea unităților cu criptare automată se pot cripta folosindu-se fie criptarea software, fie cea hardware. Criptarea hardware este mult mai rapidă decât criptarea software. Totuși, nu puteți alege ce partiții de disc doriți să criptați. Întregul disc, inclusiv orice partiții de pe acesta, vor fi criptate.

Pentru a cripta anumite partiții, trebuie să utilizați criptarea software. Asigurați-vă că ați debifat caseta **Only allow hardware encryption for Self-Encrypting Drives (SEDs)** [Permiteți numai criptarea hardware pentru unitățile cu criptare automată (SED)].

Urmați pașii de mai jos pentru a activa Drive Encryption pentru unitățile cu criptare automată:

1. Lansați **Drive Encryption**. Pentru mai multe informaţii, consultaţi Deschiderea Drive Encryption, la pagina 30.
2. Selectați caseta de bifare pentru unitatea pe care doriți să o criptați și apoi efectuați clic pe sau atingeți **Cheie de rezervă**.

NOTĂ: Pentru o mai bună securitate, selectați caseta de bifare **Disable Sleep Mode for added security** (Dezactivare mod repaus pentru o securitate sporită). Atunci când dezactivați modul repaus, nu există niciun risc ca acreditările folosite pentru deblocarea unității să fie stocate în memorie.

3. Selectați una sau mai multe dintre opțiunile de copiere de rezervă și apoi efectuați clic pe sau atingeți **Copiere de rezervă**. Pentru mai multe informaţii, consultaţi Copierea de rezervă a cheilor de criptare, la pagina 34.

4. Puteți continua să lucrați în timp ce se execută copierea de rezervă a cheii de criptare. Nu reporniți computerul.

NOTĂ: Pentru unitățile cu criptare automată, vi se va solicita să închideți computerul.

Pentru mai multe informații, consultați secțiunea de Ajutor a software-ului HP Client Security.

Dezactivarea Drive Encryption

1. Lansați **Drive Encryption**. Pentru mai multe informaţii, consultaţi Deschiderea Drive Encryption, la pagina 30.

2. Debifați caseta de bifare pentru toate unitățile criptate și apoi efectuați clic pe sau atingeți **Aplicare**.

   Dezactivarea Drive Encryption începe.

NOTĂ: Dacă s-a folosit criptarea software, se va lansa decriptarea. Aceasta poate dura mai multe ore, în funcție de dimensiunea partiției/partițiilor criptate de pe unitatea de disc. Atunci când s-a finalizat decriptarea, se dezactivează Drive Encryption.

Dacă s-a folosit criptarea hardware, atunci unitatea este decriptată instantaneu și, după câteva minute, Drive Encryption se dezactivează.

Odată ce s-a dezactivat Drive Encryption, vi se va solicita să închideți computerul, dacă a fost criptat hardware, sau să reporniți computerul, dacă a fost criptat software.

Conectarea după activarea Drive Encryption

Atunci când porniți computerul după activarea Drive Encryption și după ce contul dvs. de utilizator a fost înregistrat, trebuie să vă conectați din ecranul de conectare Drive Encryption:

NOTĂ: Atunci când computerul revine din modul Repaus sau În așteptare, autentificarea prealabilă încărcării Drive Encryption nu este afișată pentru criptarea software sau hardware. Criptarea hardware oferă opțiunea **Disable sleep mode for increased security** (Dezactivare mod repaus pentru o securitate sporită), care împiedică intrarea computerului în modurile Repaus sau În așteptare atunci când este activată.

Atunci când computerul revine din modul Hibernare, autentificarea prealabilă încărcării Drive Encryption este afișată pentru criptarea software sau hardware.

NOTĂ: Dacă administratorul Windows a activat securitatea la preîncărcare BIOS în HP Client Security și dacă HP One-Step Logon este activat (în mod predefinit), vă puteți conecta la computer imediat după autentificarea la pre-încărcarea BIOS, fără a fi nevoie să vă re-autentificați și pe ecranul de conectare Drive Encryption.

Conectarea unui singur utilizator:

- În pagina **Conectare**, tastați-vă parola Windows, PIN-ul smart cardului, SpareKey sau trageți cu degetele înregistrate.

Conectarea mai multor utilizatori:

1. În pagina **Select user to logon** (Selectați utilizatorul pentru conectare), selectați utilizatorul cu care doriți să vă conectați din lista verticală și apoi efectuați clic pe sau atingeți **Următorul**.
2. În pagina **Conectare**, tastați-vă parola Windows sau PIN-ul smart cardului sau trageți cu degetele înregistrate.

NOTĂ: Sunt acceptate următoarele smart carduri:

Smart carduri acceptate

- Gemalto Cyberflex Access 64k V2c

NOTĂ: Dacă tasta de recuperare este folosită pentru conectarea la ecranul de conectare Drive Encryption, sunt necesare acreditări suplimentare la conectarea Windows pentru a accesa conturile de utilizator.

Criptarea unor unități de disc suplimentare

Se recomandă să folosiți HP Drive Encryption pentru a vă proteja datele prin criptarea unității dvs. de disc. După activare, orice unități de disc sau partiții create pot fi criptate prin parcurgerea acestor etape:

1. Lansați **Drive Encryption**. Pentru mai multe informaţii, consultaţi Deschiderea Drive Encryption, la pagina 30.
2. Pentru unitățile criptate software, selectați partițiile unităților pe care doriți să le criptați.

NOTĂ: Aceasta se aplică și în cazul în care există mai multe tipuri de unități, anume una sau mai multe unități de disc standard și una sau mai multe unități cu criptare automată.

– sau –

▲ Pentru unitățile criptate hardware, selectați partiția/partițiile suplimentare pe care doriți să le criptați.

Sarcini avansate

Gestionarea Drive Encryption (sarcină de administrator)

Administratorii pot utiliza Drive Encryption pentru a vizualiza și modifica starea criptării (necriptat sau criptat) tuturor unităților de disc de pe computer.

- Dacă starea este „activată”, Drive Encryption a fost activat și configurat. Unitatea este într-una din următoarele situații:

Criptare software

  - Necriptat
  - Criptat
  - În curs de criptare
  - În curs de decriptare

Criptare hardware

- Criptat
- Necriptat (pentru unități suplimentare)

Criptarea sau decriptarea partițiilor individuale ale unității (numai pentru criptarea software)

Administratorii pot utiliza Drive Encryption pentru a cripta una sau mai multe partiții de pe unitatea de disc a computerului sau pentru a decripta orice partiții ale unității, care au fost deja criptate.

1. Lansați **Drive Encryption**. Pentru mai multe informaţii, consultaţi Deschiderea Drive Encryption, la pagina 30.
2. Din **Drive Status** (Stare unitate), selectați sau deselectați caseta de bifare de lângă partiția fiecărei unități de disc pe care doriți să o criptați sau decriptați și apoi efectuați clic pe sau atingeți **Aplicare**.

NOTĂ: Atunci când se criptează sau decriptează o partiție, o bară de evoluție afișează procentul din partiție care a fost criptat.

NOTĂ: Partițiile dinamice nu sunt acceptate. Dacă o partiție este afișată ca fiind disponibilă, însă nu poate fi criptată atunci când este selectată, partiția este dinamică. O partiție dinamică rezultă din micșorarea unei partiții pentru a se crea o nouă partiție în cadrul Gestionare disc.

Se afișează un avertisment dacă partiția va fi transformată în partiție dinamică.

Gestionare disc

- **Pseudonim**—Pentru o identificare mai ușoară, le puteți aloca nume unităților sau partițiilor dvs.
- **Disconnected drives** (Unități deconectate)—Drive Encryption poate identifica discurile care sunt îndepărtate din computer. Un disc care este îndepărtat din computer va fi mutat în mod automat în lista Deconectat. Dacă discul se reconectează la sistem, va apărea din nou în lista Conectat.
- Dacă nu mai doriți să urmăriți sau să gestionați unitățile deconectate, puteți șterge unitatea deconectată din lista Deconectat.
- Drive Encryption rămâne activat până ce casetele de bifare aferente tuturor unităților conectate sunt debifate, iar lista Deconectat este goală.

Copiere de rezervă și recuperare (sarcină de administrator)

Atunci când se activează Drive Encryption, administratorii pot utiliza pagina de copiere de rezervă a cheii de criptare pentru a efectua o copie de rezervă a cheilor de recuperare pe suporturi amovibile și pentru a efectua o recuperare.

Copierea de rezervă a cheilor de criptare

Administratorii pot efectua copii de rezervă ale cheii de criptare pentru o unitate criptată, pe un dispozitiv de stocare amovibil.

ATENŢIE: Asigurați-vă că dispozitivul de stocare ce conține cheia de rezervă este păstrat într-un loc sigur, deoarece, dacă ați uitat parola, dacă vă pierdeți smart cardul sau dacă nu aveți niciun deget înregistrat, acest dispozitiv vă oferă singura modalitate de acces la computer. Locul de păstrare ar trebui să fie securizat, deoarece dispozitivul de stocare permite accesul la Windows.

1. Lansați **Drive Encryption**. Pentru mai multe informaţii, consultaţi Deschiderea Drive Encryption, la pagina 30.
2. Selectați caseta de bifare pentru o unitate, apoi efectuați clic pe sau atingeți **Cheie de rezervă**.
3. Din **Create HP Drive Encryption recovery key** (Creare cheie de recuperare pentru HP Drive Encryption) selectați una sau mai multe dintre opțiunile următoare:
   - **Removable Storage** (Stocare amovibilă)—Selectați caseta de bifare și apoi selectați dispozitivul de stocare unde se va salva cheia de criptare.
   - **SkyDrive**—Selectați caseta de bifare. Trebuie să fiți conectat la internet. Conectați-vă la Microsoft SkyDrive și apoi efectuați clic pe sau atingeți **Da**.

     NOTĂ: Pentru a utiliza cheia de rezervă HP Drive Encryption stocată în SkyDrive, trebuie să o descărcați mai întâi din SkyDrive pe un dispozitiv de stocare amovibil și apoi să introduceți dispozitivul de stocare în acest computer.
   - **TPM** (numai modelele selectate) - Vă permite să vă recuperați datele utilizându-vă parola TPM.

     ATENŢIE: Dacă TPM s-a șters sau computerul este avariat, veți pierde accesul la copia de rezervă. Dacă se selectează această metodă, trebuie să se mai selecteze și o altă metodă de copiere de rezervă.
4. Efectuați clic pe sau atingeți **Copiere de rezervă**.

   Cheia de criptare se salvează pe dispozitivul de stocare pe care l-ați selectat.

Recuperarea accesului la un computer activat folosind cheile de rezervă

Administratorii pot efectua o recuperare folosind cheia Drive Encryption copiată pe un dispozitiv de stocare amovibil în momentul activării sau selectând opțiunea **Cheie de rezervă** din Drive Encryption.

1. Introduceți dispozitivul de stocare amovibil care conține cheia dvs. de rezervă.
2. Porniţi computerul.
3. Atunci când se deschide caseta de dialog pentru conectarea la HP Drive Encryption, efectuați clic pe sau atingeți **Recuperare**.
4. Tastați calea sau denumirea fișierului care conține cheia dvs. de rezervă și apoi efectuați clic pe sau atingeți **Recuperare**.
5. Atunci când se deschide caseta de dialog pentru confirmare, efectuați clic pe sau atingeți **OK**.

   Se afișează ecranul de conectare Windows.

NOTĂ: Dacă tasta de recuperare este folosită pentru conectarea la ecranul de conectare Drive Encryption, sunt necesare acreditări suplimentare la conectarea Windows pentru a accesa conturile de utilizator. Se recomandă să vă resetați parola după ce ați efectuat o recuperare.

Efectuarea unei recuperări HP SpareKey

Pentru a realiza o recuperare SpareKey din preîncărcarea Drive Encryption, va trebui să răspundeți corect la întrebările de securitate înainte de a putea accesa computerul. Pentru mai multe informații

despre configurarea recuperării SpareKey, consultați secțiunea Ajutor din software-ul HP Client Security.

Pentru a realiza o recuperare HP SpareKey dacă ați uitat parola:

1. Porniţi computerul.
2. Atunci când se afișează pagina HP Drive Encryption, navigați la pagina de conectare a utilizatorului.
3. Faceţi clic pe **SpareKey**.

   NOTĂ: Dacă SpareKey-ul dvs. nu a fost inițializat în HP Client Security, butonul **SpareKey** nu este disponibil.

4. Tastați răspunsurile corecte la întrebările afișate și apoi efectuați clic pe **Conectare**.

   Se afișează ecranul de conectare Windows.

NOTĂ: Dacă se folosește SpareKey pentru conectarea la ecranul Drive Encryption, sunt necesare acreditări suplimentare la conectarea Windows pentru a accesa conturile de utilizator. Se recomandă să vă resetați parola după ce ați efectuat o recuperare.

6 HP File Sanitizer (numai la anumite modele)

File Sanitizer vă permite să distrugeţi datele în siguranţă (de exemplu: informații personale sau fișiere, date istorice sau Web sau alte componente ale datelor) de pe unitatea de disc internă a computerului și să curățați periodic unitatea de disc internă a computerului.

File Sanitizer nu poate fi utilizat pentru curățarea următoarelor tipuri de unități:

- Unitățile SSD, inclusiv volumele RAID care extind un dispozitiv SSD
- Unitățile externe conectate prin interfețe USB, Firewire sau eSATA

Dacă se încearcă o operațiune de distrugere sau curățare pe un SSD, se afișează un mesaj de avertizare, iar operațiunea nu se execută.

Distrugere

Distrugerea este diferită de acțiunea Windows® standard de ștergere. Atunci când distrugeți date folosind File Sanitizer, fișierele sunt suprascrise cu date fără sens, fapt care face imposibilă recuperarea datelor originale. O acțiune simplă de ștergere în Windows poate lăsa fișierul sau datele intacte pe unitatea de disc, sau într-o stare în care se pot utiliza anumite metode de investigare pentru a le recupera.

Puteți programa un moment ulterior la care să se efectueze distrugerea sau puteți activa manual distrugerea prin selectarea pictogramei **File Sanitizer** din ecranul de întâmpinare HP Client Security sau folosind pictograma **File Sanitizer** de pe desktopul Windows. Pentru mai multe informaţii, consultați Configurarea unui program de distrugere, la pagina 39, Distrugere cu clic dreapta, la pagina 41 sau Demararea manuală a unei operațiuni de distrugere, la pagina 41.

NOTĂ: Un fișier .dll este distrus și eliminat din sistem numai dacă a fost mutat în Coșul de reciclare.

Curăţarea spaţiului liber

Ștergerea de date în Windows nu elimină în totalitate conținutul acestora de pe unitatea de disc. Windows șterge numai referința la date sau locul unde respectivele date se află pe unitatea de disc. Conținutul datelor rămâne în continuare pe unitatea de disc până ce alte date suprascriu aceeași zonă de pe unitatea de disc.

Curățarea spațiului liber vă permite să scrieți în mod securizat date aleatorii peste date șterse, fapt care împiedică vizualizarea de către utilizatori a conținutului original al datelor șterse.

NOTĂ: Curățarea spațiului liber nu oferă o securitate suplimentară datelor distruse.

Puteți stabili un moment ulterior la care să se efectueze curățarea spațiului liber sau puteți activa manual curățarea spațiului liber prin selectarea pictogramei **File Sanitizer** din ecranul de întâmpinare HP Client Security sau folosind pictograma **File Sanitizer** de pe desktopul Windows. Pentru mai multe informaţii, consultați Configurarea unui program de curățare a spațiului liber, la pagina 40, Demararea manuală a curățării spațiului liber, la pagina 42 sau Utilizarea pictogramei File Sanitizer, la pagina 41.

Deschiderea File Sanitizer

1. Din ecranul Pornire, efectuați clic pe sau atingeți aplicația **HP Client Security** (Windows 8).

   – sau –

   De pe desktop-ul Windows, efectuați dublu clic pe sau atingeți de două ori pictograma **HP Client Security** din zona de notificare, aflată în extrema dreaptă a barei de sarcini.

2. Din **Data**, efectuați clic pe sau atingeți **File Sanitizer**.

– sau –

▲ Efectuați dublu clic pe sau atingeți de două ori pictograma **File Sanitizer** de pe desktopul Windows.

– sau –

▲ Efectuați clic dreapta sau atingeți și mențineți apăsată pictograma **File Sanitizer** de pe desktopul Windows și apoi selectați **Open File Sanitizer** (Deschidere File Sanitizer).

Procedurile de configurare

Shredding (Distrugere)- File Sanitizer șterge sau distruge în condiții sigure categoriile de date selectate.

1. Din **Shredding** (Distrugere), selectați caseta de bifare pentru fiecare tip de fișier care trebuie distrus sau debifați caseta dacă nu doriți să distrugeți respectivele fișiere.

   - **Coșul de reciclare**—Distruge toate elementele din interiorul Coșului de reciclare.
   - **Temporary system files** (Fișiere temporare de sistem)—Distruge toate fișierele care se găsesc în folderul temporar al sistemului. Următoarele variabile de mediu sunt căutate în ordinea următoare, iar prima cale găsită este considerată ca fiind folderul de sistem:
     - TMP
     - TEMP
   - **Fișiere temporare de internet**—Distruge copiile paginilor web, imaginilor și materialelor media salvate de browserele web, pentru o vizualizare mai rapidă.
   - **Cookies** (Module cookie)—Distruge toate fișierele stocate pe un computer de site-urile web pentru a salva preferințele, precum informațiile de conectare.

2. Pentru a demara distrugerea, efectuați clic pe sau atingeți **Shred** (Distruge).

Bleaching (Curățare)—Scrie date aleatorii pe spațiul liber și împiedică recuperarea elementelor șterse.

▲ Pentru a demara curățarea, efectuați clic pe sau atingeți **Bleach** (Curăță).

Opțiuni File Sanitizer—Selectați caseta de bifare pentru a activa fiecare dintre următoarele opțiuni, sau deselectați-o pentru a dezactiva o opțiune:

- **Enable Desktop icon** (Activare pictogramă desktop)—Afișează pictograma File Sanitizer pe desktopul Windows.
- **Enable right-click** (Activare clic dreapta)—Vă permite să efectuați clic dreapta pe sau să atingeți și să mențineți apăsat un element și apoi să selectați **HP File Sanitizer – Shred** (HP File Sanitizer - Distrugere).

- **Ask for Windows password before manual shredding** (Solicită parola Windows înainte de distrugerea manuală)—Necesită autentificare cu parola Windows înainte de a distruge manual un element.
- **Shred Cookies and Temporary Internet Files on browser close** (Distruge modulele cookie și fișierele temporare de internet la închiderea browser-ului)—Distruge toate datele selectate privind navigarea pe internet, precum istoricul URL al browser-ului, în momentul în care închideți un browser Web.

Configurarea unui program de distrugere

Puteți planifica o oră la care doriți să se efectueze în mod automat distrugerea sau puteți să distrugeți datele manual, în orice moment. Pentru mai multe informaţii, consultaţi Procedurile de configurare, la pagina 38.

1. Deschideți File Sanitizer și apoi efectuați clic pe sau atingeți **Configurări**.
2. Pentru a planifica un moment ulterior la care doriți să distrugeți datele selectate, din **Shred Schedule** (Program de distrugere) selectați **Niciodată**, **O dată**, **Zilnic**, **Săptămânal** sau **Lunar** și apoi selectați o dată și o oră:
   a. Efectuați clic pe sau atingeți câmpul oră, minut sau AM/PM.
   b. Derulați până ce se afișează valoarea dorită la același nivel ca și celelalte câmpuri.
   c. Efectuați clic pe sau atingeți spațiul alb care înconjoară câmpurile cu configurările temporale.
   d. Repetați pentru fiecare câmp până ce s-a selectat programul corect.
3. Se afișează următoarele patru tipuri de date:
   - **Coșul de reciclare**—Distruge toate elementele din interiorul Coșului de reciclare.
   - **Temporary system files** (Fișiere temporare de sistem)—Distruge toate fișierele care se găsesc în folderul temporar al sistemului. Următoarele variabile de mediu sunt căutate în ordinea următoare, iar prima cale găsită este considerată ca fiind folderul de sistem:
     - TMP
     - TEMP
   - **Fișiere temporare de internet**—Distruge copiile paginilor web, imaginilor și materialelor media salvate de browserele web, pentru o vizualizare mai rapidă.
   - **Cookies** (Module cookie)—Distruge toate fișierele stocate pe un computer de site-urile web pentru a salva preferințele, precum informațiile de conectare.

   Dacă sunt bifate, acest tip de date sunt distruse la momentul planificat.
4. Pentru a selecta date suplimentare, personalizate, pe care doriți să le distrugeți:
   a. Din **Scheduled Shred List** (Listă de distrugere planificată), efectuați clic pe sau atingeți **Adăugare folder** și apoi navigați la fișier sau la folder.
   b. Efectuați clic pe sau atingeți **Deschidere** și apoi efectuați clic pe sau atingeți **OK**.

   Pentru a elimina elemente din lista de distrugere planificată, debifați caseta de bifare aferentă respectivelor elemente.

Configurarea unui program de curățare a spațiului liber

Curățarea spațiului liber nu oferă o securitate suplimentară datelor distruse.

1. Deschideți File Sanitizer și apoi efectuați clic pe sau atingeți **Configurări**.
2. Pentru a planifica un moment ulterior la care doriți să vă curățați unitatea de disc, din Bleach Schedule **(Program de curăţare)**, selectaţi **Niciodată**, **O dată**, **ZilnicSăptămânal** sau **Lunar** şi apoi selectaţi o dată şi o oră.
   a. Efectuați clic pe sau atingeți câmpul oră, minut sau AM/PM.
   b. Derulați până ce se afișează ora dorită la același nivel ca și celelalte câmpuri.
   c. Efectuați clic pe sau atingeți spațiul alb care înconjoară câmpurile cu configurările temporale.
   d. Repetați până ce s-a selectat programul corect.

NOTĂ: Operațiunea de curățare a spațiului liber poate dura mult timp. Asigurați-vă că ați conectat computerul la o sursă de curent alternativ. Deși curățarea spațiului liber se derulează în fundal, utilizarea mai intensă a procesorului poate afecta performanța computerului dvs. Curățarea spațiului liber se poate efectua după programul de lucru sau atunci când nu folosiți computerul.

Protejarea fișierelor împotriva distrugerii

Pentru a proteja fișierele sau folderele împotriva distrugerii:

1. Deschideți File Sanitizer și apoi efectuați clic pe sau atingeți **Configurări**.
2. Din **Never Shred List** (Lista cu elemente care nu trebuie distruse niciodată), efectuați clic pe sau atingeți **Adăugare folder** și apoi navigați la fișier sau la folder.
3. Efectuați clic pe sau atingeți **Deschidere** și apoi efectuați clic pe sau atingeți **OK**.

NOTĂ: Fișierele din această listă sunt protejate atâta timp cât rămân pe listă.

Pentru a elimina elemente din lista de excluderi, debifați caseta de bifare aferentă respectivelor elemente.

Activităţi generale

Utilizați File Sanitizer pentru a efectua următoarele sarcini:

- **Utilizați pictograma File Sanitizer pentru a iniția distrugerea**—Trageți fișierele pe pictograma **File Sanitizer** de pe desktop-ul Windows. Pentru mai multe detalii, consultați Utilizarea pictogramei File Sanitizer, la pagina 41.
- **Distrugeți manual un element specific sau toate elementele selectate**—Distrugeți în orice moment elemente fără a aștepta ora planificată de distrugere. Pentru mai multe detalii, consultați Distrugere cu clic dreapta, la pagina 41 sau Demararea manuală a unei operațiuni de distrugere, la pagina 41.
- **Activați manual curățarea spațiului liber**—Activați în orice moment curățarea spațiului liber. Pentru mai multe detalii, consultați Demararea manuală a curățării spațiului liber, la pagina 42.
- **Vizualizați fișierele jurnal**—Vizualizați fișierele jurnal aferente distrugerii sau curățării spațiului liber, care conțin orice erori sau defecțiuni apărute pe durata celei mai recente operațiuni de distrugere sau curățare a spațiului liber. Pentru mai multe detalii, consultați Vizualizarea fișierelor jurnal, la pagina 42.

NOTĂ: Operațiunea de distrugere sau de curățare a spațiului liber poate dura mult timp. Deși distrugerea și curățarea spațiului liber se derulează în fundal, utilizarea mai intensă a procesorului poate afecta performanța computerului dvs.

Utilizarea pictogramei File Sanitizer

ATENŢIE: Elementele distruse nu pot fi recuperate. Analizați cu atenție ce elemente selectați pentru distrugere manuală.

Atunci când demarați manual o operațiune de distrugere, lista standard de distrugere din ecranul File Sanitizer este distrusă (a se vedea Procedurile de configurare, la pagina 38).

Puteți demara manual o operațiune de distrugere într-unul din modurile următoare:

1. Deschideți File Sanitizer (a se vedea Deschiderea File Sanitizer, la pagina 38) și apoi efectuați clic pe sau atingeți **Shred** (Distruge).
2. Atunci când se deschide caseta de dialog pentru confirmare, asigurați-vă că elementele pe care doriți să le distrugeți sunt bifate și apoi efectuați clic pe sau atingeți **OK**.

– sau –

1. Efectuați clic dreapta sau atingeți și mențineți apăsată pictograma **File Sanitizer** de pe desktopul Windows și apoi efectuați clic pe sau atingeți **Shred Now** (Distruge acum).
2. Atunci când se deschide caseta de dialog pentru confirmare, asigurați-vă că elementele pe care doriți să le distrugeți sunt bifate și apoi efectuați clic pe sau atingeți **Shred** (Distruge).

Distrugere cu clic dreapta

ATENŢIE: Elementele distruse nu pot fi recuperate. Analizați cu atenție ce elemente selectați pentru distrugere manuală.

Dacă s-a selectat **Enable right-click shredding** (Activare distrugere cu clic dreapta) din ecranul File Sanitizer, puteți distruge un element după cum urmează:

1. Navigați la documentul sau la folderul pe care doriți să-l distrugeți.
2. Efectuați clic dreapta sau atingeți și mențineți apăsat fișierul sau folderul și apoi selectați **HP File Sanitizer – Shred** (HP File Sanitizer - Distrugere).

Demararea manuală a unei operațiuni de distrugere

ATENŢIE: Elementele distruse nu pot fi recuperate. Analizați cu atenție ce elemente selectați pentru distrugere manuală.

Atunci când demarați manual o operațiune de distrugere, lista standard de distrugere din ecranul File Sanitizer este distrusă (a se vedea Procedurile de configurare, la pagina 38).

Puteți demara manual o operațiune de distrugere într-unul din modurile următoare:

1. Deschideți File Sanitizer (a se vedea Deschiderea File Sanitizer, la pagina 38) și apoi efectuați clic pe sau atingeți **Shred** (Distruge).
2. Atunci când se deschide caseta de dialog pentru confirmare, asigurați-vă că elementele pe care doriți să le distrugeți sunt bifate și apoi efectuați clic pe sau atingeți **OK**.

– sau –

1. Efectuați clic dreapta sau atingeți și mențineți apăsată pictograma **File Sanitizer** de pe desktopul Windows și apoi efectuați clic pe sau atingeți **Shred Now** (Distruge acum).
2. Atunci când se deschide caseta de dialog pentru confirmare, asigurați-vă că elementele pe care doriți să le distrugeți sunt bifate și apoi efectuați clic pe sau atingeți **Shred** (Distruge).

Demararea manuală a curățării spațiului liber

Atunci când demarați manual o operațiune de curățare, lista standard de distrugere din ecranul File Sanitizer este curățată (a se vedea Procedurile de configurare, la pagina 38).

Puteți demara manual o operațiune de curățare într-unul din modurile următoare:

1. Deschideți File Sanitizer (a se vedea Deschiderea File Sanitizer, la pagina 38) și apoi efectuați clic pe sau atingeți **Bleach** (Curățăț).
2. Atunci când se deschide caseta de dialog pentru confirmare, efectuați clic pe sau atingeți **OK**.

– sau –

1. Efectuați clic dreapta sau atingeți și mențineți apăsată pictograma **File Sanitizer** de pe desktopul Windows și apoi efectuați clic pe sau atingeți **Bleach Now** (Curățăț acum).
2. Atunci când se deschide caseta de dialog pentru confirmare, efectuați clic pe sau atingeți **Bleach** (Curățare).

Vizualizarea fișierelor jurnal

De fiecare dată când se derulează o operațiune de distrugere sau de curățare a spațiului liber, se generează fișiere jurnal care includ orice erori sau defecțiuni. Fișierele jurnal sunt întotdeauna actualizate în conformitate cu cea mai recentă operațiune de distrugere sau curățare a spațiului liber.

NOTĂ: Fișierele care au fost distruse sau curățate cu succes nu apar în fișierele jurnal.

Pentru operațiunile de distrugere se creează un fișier jurnal, și un altul pentru operațiunile de curățare a spațiului liber. Ambele fișiere jurnal se află pe unitatea de disc, în următoarele foldere:

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

Pentru sistemele pe 64 de biți, fișierele jurnal se află pe unitatea de disc, în următoarele foldere:

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

7 HP Device Access Manager (numai la anumite modele)

HP Device Access Manager controlează accesul la date prin dezactivarea serviciilor de transfer de date.

NOTĂ: Unele dispozitive de interfață umană sau dispozitive de intrare, precum mouse, tastatură, Zonă de atingere şi cititor de amprente, nu sunt controlate de Device Access Manager. Pentru mai multe informaţii, consultaţi Clase de dispozitive negestionate, la pagina 46.

Administratorii de sisteme de operare Windows® folosesc HP Device Manager pentru a controla accesul la dispozitivele de pe un sistem și pentru a proteja împotriva accesului neautorizat:

- Profilurile dispozitivului sunt create pentru fiecare utilizator, pentru a defini dispozitivele la care li se permite sau refuză accesul.
- Autentificarea JITA (Just In Time) le permite utilizatorilor predefiniți să se autentifice pentru a accesa dispozitivele la care altminteri li se refuză accesul.
- Administratorii şi utilizatorii de încredere pot fi excluşi de la restricţiile legate de accesul la dispozitiv ce au fost impuse de Device Access Manager prin adăugarea lor la grupul de administratori al dispozitivului. Apartenenţa la acest grup este gestionată cu ajutorul Setări avansate.
- Accesul la dispozitive poate fi permis sau refuzat pe baza apartenenței la grup sau pentru utilizatorii individuali.
- Pentru clasele de dispozitive precum unităţile CD-ROM şi unităţile DVD, accesul pentru citire şi scriere poate fi acordat sau refuzat separat.

HP Device Access Manager este configurat în mod automat cu următoarele setări, pe durata executării expertului de configurare HP Client Security:

- Suporturile amovibile cu autentificare JITA sunt activate pentru administratori și utilizatori.
- Politica dispozitivului permite accesul complet la alte dispozitive.

Deschiderea Device Access Manager

1. Din ecranul Pornire, efectuați clic pe sau atingeți aplicația **HP Client Security** (Windows 8).

   – sau –

   De pe desktop-ul Windows, efectuați dublu clic pe sau atingeți de două ori pictograma **HP Client Security** din zona de notificare, aflată în extrema dreaptă a barei de sarcini.

2. Din **Dispozitiv**, efectuați clic pe sau atingeți **Device Permissions** (Permisiuni dispozitiv).

   - Utilizatorii standard pot vizualiza accesul lor la momentul de față la respectivul dispozitiv (a se vedea Vizualizare utilizator, la pagina 44).
   - Administratorii pot vizualiza și pot efectua modificări asupra accesului la dispozitiv, care este configurat pentru computer la momentul respectiv, prin efectuarea unui clic pe sau prin atingerea filei **Modificare** și introducând apoi parola de administrator (a se vedea Vizualizare sistem, la pagina 44).

Vizualizare utilizator

Atunci când se selectează **Device Permissions** (Permisiuni dispozitiv), se afișează Vizualizare utilizator. În funcție de politică, utilizatorii standard și administratorii își pot vedea propriul acces la clasele de dispozitive sau la dispozitivele individuale de pe acest computer.

- **Current user** (Utilizator curent)—Se afișează numele utilizatorului care este conectat la momentul respectiv.
- **Device Class** (Clasă dispozitiv)—Sunt afișate tipurile de dispozitive.
- **Acces**—Se afișează accesul dvs., configurat la momentul respectiv, la tipurile de dispozitive sau la dispozitivele specifice.
- **Durată**—Se afișează limita temporală a accesului dvs. la unitățile CD/DVD-ROM sau la unitățile de disc amovibile.
- **Configurări**—Administratorii pot schimba unitățile al căror acces este controlat de Device Access Manager.

Vizualizare sistem

Din modul de vizualizare Sistem, administratorii pot permite sau refuza accesul la dispozitivele de pe acest computer pentru grupul de utilizatori sau grupul de administratori.

▲ Administratorii pot accesa modul de vizualizare Sistem efectuând clic pe sau atingând **Modificare**, tastând parola de administrator și apoi selectând una dintre următoarele opțiuni:

- **Device Access Manager**—Pentru a porni sau opri HP Device Access Manager cu autentificare JITA, efectuați clic pe sau atingeți **Pornit** sau **Oprit**.
- **Users and groups on this PC** (Utilizatori și grupuri pe acest PC)—Afișează grupul de utilizatori sau grupul de administratori cărora li se permite sau refuză accesul la clasele de dispozitive selectate.
- **Clasă de dispozitive**—Afișează clasele de dispozitive și dispozitivele care sunt instalate pe sistem sau care au fost instalate anterior pe sistem. Pentru a extinde lista, efectuați clic pe pictograma **+**. Se afișează toate dispozitivele conectate la computer, iar grupul de administratori și de utilizatori se extinde pentru a arăta apartenența acestora. Pentru a reîmprospăta lista de dispozitive, efectuați clic pe pictograma cu o săgeată rotundă (reîmprospătare).
  - Protecția se aplică de obicei pentru o clasă de dispozitive. Dacă accesul este configurat în modul **Permis**, atunci utilizatorul sau grupul selectat va putea să acceseze orice dispozitiv din respectiva clasă de dispozitive.
  - Protecția se poate aplica și unor dispozitive specifice.
  - Configurați autentificarea JITA permițându-le utilizatorilor selectați să aibă acces la unitățile DVD/CD-ROM sau la unitățile de disc amovibil, dacă se autentifică. Pentru mai multe informaţii, consultaţi Configurație JITA, la pagina 45.
  - Permiteți sau refuzați accesul la alte clase de dispozitive, precum suporturi amovibile (de exemplu unități flash USB), porturi seriale și paralele, dispozitive Bluetooth®, dispozitive tip modem, dispozitive PCMCIA/ExpressCard, dispozitive 1394, cititor de amprente și cititor de smart card. Dacă cititorul de amprente și cititorul de smart card sunt refuzate, acestea se pot utiliza ca și acreditări de autentificare, însă nu pot fi folosite la nivelul politicii de sesiune.

NOTĂ: Dacă dispozitivele Bluetooth sunt folosite ca și acreditări de autentificare, accesul la dispozitivele Bluetooth nu ar trebuie să fie restricționat prin politica Device Access Manager.

- Atunci când selectați o configurație la nivelului grupului sau dispozitivului și sunteți întrebat dacă doriți să aplicați configurația la obiectele subordonate:

  Da—Configurația se va propaga.

  Nu—Configurația nu se va propaga.

- Unele clase de dispozitive, precum DVD și CD-ROM, pot fi controlate suplimentar prin permiterea sau refuzarea accesului separat pentru operațiunile de citire și scriere.

NOTĂ: Grupul de administratori nu se poate adăuga la lista de utilizatori.

- **Acces**—Efectuați clic pe sau atingeți săgeata jos și apoi selectați unul din următoarele tipuri de acces pentru a permite sau refuza accesul:
  - **Permis - acces complet**
  - **Permis - numai citire**
  - **Permis - Autentificare JITA necesară**—Pentru mai multe informaţii, a se vedea Configurație JITA, la pagina 45.

    Dacă se selectează acest tip de acces, din **Durată**, efectuați clic pe sau atingeți săgeata jos pentru a selecta o limită temporală.
  - **Refuzat**
- **Durată**—Efectuați clic pe sau atingeți săgeata jos pentru a selecta o limită temporală pentru accesul la dispozitivele CD/DVD-ROM sau la unitățile de disc amovibil (a se vedea Configurație JITA, la pagina 45).

Configurație JITA

Configurația JITA îi permite administratorului să vizualizeze și să modifice lista de utilizatori și grupuri cărora li se permite accesul la dispozitive folosind autentificarea JITA.

Utilizatorii care beneficiază de autentificare JITA vor putea accesa anumite dispozitive pentru care politicile create în modul de vizualizare **Device Class Configuration** (Configurație clasă de dispozitive) au fost restricționate.

Perioada JITA poate fi autorizată pentru un număr stabilit de minute sau pentru o perioadă nelimitată. Utilizatorii cu acces JITA nelimitat vor putea accesa dispozitivul din momentul în care se autentifică până în momentul în care s-au deconectat din sistem.

Dacă utilizatorul primește o perioadă de autentificare JITA limitată, utilizatorul va fi întrebat dacă dorește să-și extindă accesul, cu un minut înainte de expirarea perioadei JITA. De îndată ce utilizatorul se deconectează din sistem sau în momentul în care un alt utilizator se conectează, perioada JITA expiră. Următoarea dată când utilizatorul se conectează și încearcă să acceseze un dispozitiv cu JITA activată, se afișează o casetă în care vor trebui tastate acreditările.

JITA este disponibilă pentru următoarele clase de dispozitive:

- Unități DVD/CD-ROM
- Unități de disc amovibil

Crearea unei politici JITA pentru un utilizator sau un grup

Administratorii le pot permite utilizatorilor sau grupurilor să acceseze dispozitive folosind autentificarea JITA.

1. Lansați **Device Access Manager** și apoi efectuați clic pe sau atingeți **Modificare**.
2. Selectați utilizatorul sau grupul și apoi, din **Acces**, atât pentru **unitățile de disc amovibil**, cât și pentru **unitățile DVD/CD-ROM**, efectuați clic pe sau atingeți săgeata jos și apoi selectați **Permis – JITA necesară**.
3. Din secțiunea **Durată**, efectuați clic pe sau atingeți săgeata jos pentru a selecta o perioadă de timp pentru accesul JITA.

Utilizatorul trebuie să se deconecteze și apoi să se conecteze din nou pentru ca noua configurație JITA să devină aplicabilă.

Dezactivarea unei politici JITA pentru un utilizator sau un grup

Administratorii pot dezactiva accesul unui utilizator sau grup la dispozitive folosind autentificarea JITA.

1. Lansați **Device Access Manager** și apoi efectuați clic pe sau atingeți **Modificare**.
2. Selectați utilizatorul sau grupul și apoi, din **Acces**, atât pentru **unitățile de disc amovibil**, cât și pentru **unitățile DVD/CD-ROM**, efectuați clic pe sau atingeți săgeata jos și apoi selectați **Refuzat**.

Atunci când utilizatorul se conectează și încearcă să acceseze dispozitivul, accesul este refuzat.

Setări

Modul de vizualizare **Configurări** le permite administratorilor să vizualizeze și să modifice unitățile al căror acces este controlat de Device Access Manager.

NOTĂ: Device Access Manager trebuie activat atunci când lista de litere aferente unităților este configurată (a se vedea Vizualizare sistem, la pagina 44).

Clase de dispozitive negestionate

HP Device Access Manager nu gestionează următoarele clase de dispozitive:

- Dispozitive de intrare/ieșire
  - CD-ROM
  - Unitate de disc
  - Controler de dischetă (FDC)
  - Controler de hard disk (HDC)
  - Clasa de dispozitive de interfață umană (HID)
  - Dispozitive de interfață umană cu infraroșii
  - Mouse
  - Serială multi-port
  - Tastatură

- Imprimante plug-and-play (PnP)
- Imprimantă
- Îmbunătățiri (upgrade-uri) ale imprimantei

- Alimentare
  - Asistență pentru managementul avansat al energiei (APM)
  - Acumulator
- Diverse
  - Computer
  - Decodor
  - Afişaj
  - Unitate de afişare unificată Intel®
  - Legacard
  - Unitate media
  - Dispozitive schimbare mediu
  - Tehnologie memorie
  - Monitor
  - Multifuncție
  - Client net
  - Serviciu net
  - Trans. net
  - Procesor
  - Adaptor SCSI
  - Accelerator de siguranță
  - Dispozitive de siguranță
  - Sistem
  - Necunoscut
  - Volum
  - Instantaneu de volum

8 HP Trust Circles

HP Trust Circles este o aplicație de securizare a fișierelor și documentelor, care combină criptarea fișierului din folder cu o capacitate de partajare a documentelor în interiorul unui „circuit al încrederii”. Aplicația criptează fișierele plasate în folderele specificate de utilizator, protejându-le în cadrul unui așa-numit circuit al încrederii. Odată protejate, fișierele pot fi utilizate și partajate numai de către membrii din respectivul circuit al încrederii. Dacă un non-membru primește un fișier protejat, fișierul rămâne criptat, iar non-membrul nu poate avea acces la conținutul său.

Deschiderea aplicației Trust Circles

1. Din ecranul Pornire, efectuați clic pe sau atingeți aplicația **HP Client Security**.

   – sau –

   De pe desktop-ul Windows, efectuați dublu clic pe pictograma **HP Client Security** din zona de notificare, aflată în partea dreaptă a barei de sarcini.

2. Din **Date**, efectuați clic pe sau atingeți **Trust Circles**.

Noţiuni introductive

Există două modalități în care puteți trimite invitații pe e-mail și în care puteți răspunde la acestea:

- **Using Microsoft® Outlook** (Folosirea Microsoft® Outlook)—Folosirea Trust Circle împreună cu Microsoft Outlook automatizează prelucrarea oricăror invitații Trust Circle, cât și a răspunsurilor de la alți utilizatori Trust Circle.
- **Using Gmail, Yahoo, Outlook.com or other email services (SMTP)** [Folosirea Gmail, Yahoo, Outlook.com sau a altor servicii de e-mail (SMTP)]—Atunci când vă tastați numele, adresa de e-mail și parola, Trust Circles folosește serviciul dvs. de e-mail pentru a trimite invitații prin e-mail către membrii selectați pentru a se alătura circuitului dvs. al încrederii.

Pentru a vă configura profilul de bază:

1. Tastați-vă numele și adresa de e-mail, apoi efectuați clic pe sau atingeți **Următorul**.

   Numele este vizibil oricăror membri invitați să se alăture circuitului dvs. al încrederii. Adresa de e-mail este utilizată pentru a trimite, a primi sau a răspunde la invitații.

2. Tastați-vă parola aferentă contului de e-mail și apoi efectuați clic pe sau atingeți **Următorul**.

   Se va trimite un e-mail de testare, pentru a se verifica acuratețea configurărilor de e-mail.

   NOTĂ: Computerul trebuie conectat la o rețea.

3. În câmpul **Trust Circle Name** (Denumire circuit al încrederii), indicați un nume pentru respectivul circuit și apoi efectuați clic pe sau atingeți **Următorul**.

4. Adăugați membri și foldere și apoi efectuați clic pe sau atingeți **Următorul**. Astfel, s-a creat un circuit al încrederii, care include orice foldere care au fost selectate și care trimite invitații prin e-mail oricăror membri care au fost selectați. Dacă, din orice motiv, invitația nu se poate trimite, se afișează o notificare. Membrii pot fi invitați din nou, în orice moment, din modul de vizualizare Trust Circle, dacă se efectuează clic pe **Your Trust Circles** (Circuitele dvs. ale încrederii) și

apoi dublu clic sau atingere dublă pe respectivul circuit al încrederii. Pentru mai multe informaţii, consultaţi Trust Circles, la pagina 49.

Trust Circles

Puteți crea un circuit al încrederii pe durata configurării inițiale, după ce ați tastat adresa dvs. de e-mail, sau în modul de vizualizare Trust Circle:

▲ Din modul de vizualizare Trust Circle, efectuați clic pe sau atingeți **Create Trust Circle** (Creare circuit al încrederii) și apoi tastați denumirea circuitului încrederii.

- Pentru a adăuga membri în circuitul încrederii, efectuați clic pe sau atingeți pictograma **M+** de lângă **Membri** și apoi urmați instrucțiunile de pe ecran.
- Pentru a adăuga foldere în circuitul încrederii, efectuați clic pe sau atingeți pictograma **+** de lângă **Foldere** și apoi urmați instrucțiunile de pe ecran.

Adăugarea de foldere la un circuit al încrederii

Adăugarea de foldere la un nou circuit al încrederii:

- Pe durata creării unui circuit al încrederii, puteți adăuga foldere efectuând clic pe sau atingând pictograma **+** de lângă **Foldere** și apoi urmând instrucțiunile de pe ecran.

  – sau –

- În Windows Explorer, efectuați clic dreapta pe sau atingeți și țineți apăsat un folder care nu face parte la momentul respectiv dintr-un circuit al încrederii, apoi selectați **Trust Circle** și selectați **Create Trust Circle from Folder** (Creare circuit al încrederii din folder).

SFAT: Puteți selecta unul sau mai multe foldere.

Adăugarea de foldere la un circuit al încrederii existent:

- Din modul de vizualizare Trust Circle, efectuați clic pe **Your Trust Circles** (Circuitele dvs. ale încrederii), efectuați dublu clic pe sau atingeți de două ori circuitul existent al încrederii pentru a afișa folderele curente, apoi efectuați clic pe sau atingeți pictograma **+** de lângă **Foldere** și urmați instrucțiunile de pe ecran.

  – sau –

- În Windows Explorer, efectuați clic dreapta pe sau atingeți și țineți apăsat un folder care nu face parte la momentul respectiv dintr-un circuit al încrederii, apoi selectați **Trust Circle** și selectați **Add to existing Trust Circle from Folder** (Adăugare la un circuit al încrederii existent din folder).

SFAT: Puteți selecta unul sau mai multe foldere.

Odată ce un folder a fost adăugat la un circuit al încrederii, Trust Circles criptează automat folderul și conținutul acestuia. Odată ce toate folderele sunt criptate, se afișează o notificare. De asemenea, se afișează un lacăt de culoare verde pe toate pictogramele folderelor criptate și pe pictogramele fișierelor din foldere, fapt care arată că acestea sunt protejate în totalitate.

Adăugarea de membri la un circuit al încrederii

Sunt necesari trei pași pentru a adăuga membri la un circuit al încrederii:

1. **Invitație**—Mai întâi, proprietarul circuitului încrederii invită membrul/membrii. Se poate trimite un e-mail de invitație către mai mulți utilizatori sau liste/grupuri de distribuție.
2. **Acceptare**—Persoana invitată primește invitația și alege dacă o acceptă sau o refuză. Dacă acceptă invitația, persoana care lansează invitația va primi un răspuns prin e-mail. Dacă invitația a fost transmisă către un grup, fiecare membru primește o invitație și alege să o accepte sau să o refuze.
3. **Înregistrare**—Persoana care lansează invitația are ocazia finală de a decide dacă dorește să adauge membrul în circuitul încrederii. Dacă persoana care lansează invitația decide să înregistreze membrul, acesta va primi un e-mail de confirmare a răspunsului. Atât persoana care lansează, cât și cea care primește invitația, au posibilitatea de a verifica securitatea procesului de invitație. Codul de verificare este afișat pentru persoana care lansează invitația, iar acesta va trebui citit persoanei invitate la telefon. Odată ce codul a fost verificat, persoana care lansează invitația poate trimite e-mailul final de înregistrare.

Adăugarea de membri la un nou circuit al încrederii:

▲ Pe durata creării unui circuit al încrederii, puteți adăuga membri efectuând clic pe sau atingând pictograma **M+** de lângă **Membri** și apoi urmând instrucțiunile de pe ecran.

- Dacă folosiți Outlook, selectați persoanele de contact din carnetul de adrese Outlook și apoi efectuați clic pe **OK**.
- Dacă folosiți un alt serviciu de e-mail, puteți fie să adăugați manual noi adrese de e-mail la Trust Circle, fie le puteți extrage din adresele e-mail înregistrate pe Trust Circle.

Adăugarea de membri la un circuit al încrederii existent:

▲ Din modul de vizualizare Trust Circle, efectuați clic pe **Your Trust Circles** (Circuitele dvs. ale încrederii), efectuați dublu clic pe sau atingeți de două ori circuitul existent al încrederii pentru a afișa membrii actuali, apoi efectuați clic pe sau atingeți pictograma **M+** de lângă **Membri** și urmați instrucțiunile de pe ecran.

- Dacă folosiți Outlook, selectați persoanele de contact din carnetul de adrese Outlook și apoi efectuați clic pe **OK**.
- Dacă folosiți un alt serviciu de e-mail, puteți fie să adăugați manual noi adrese de e-mail la Trust Circle, fie le puteți extrage din adresele e-mail înregistrate pe Trust Circle.

Adăugarea de fișiere la un circuit al încrederii

Puteți adăuga fișiere la un circuit al încrederii într-unul din următoarele moduri:

- Copiați sau mutați fișierul într-un folder deja existent, din circuitul încrederii.

  – sau –

- În Windows Explorer, efectuați clic dreapta pe sau atingeți și țineți apăsat un fișier care nu este criptat la momentul respectiv, apoi selectați **Trust circle** şi selectaţi **Criptare**. Vi se va solicita să selectați circuitul încrederii în care ar trebui să fie adăugat fișierul.

SFAT: Puteți selecta unul sau mai multe fișiere.

Foldere criptate

Orice membru al unui circuit al încrederii poate vizualiza și modifica fișierele care aparțin respectivului circuit al încrederii.

NOTĂ: Managerul/cititorul Trust Circle nu sincronizează fișierele între membri.

Fișierele trebuie partajate prin metodele existente, precum e-mail, ftp sau furnizori de servicii de stocare în cloud. Fișierele copiate în, mutate în sau create în cadrul unui folder dintr-un circuit al încrederii sunt protejate imediat.

Eliminarea de foldere dintr-un circuit al încrederii

Eliminarea unui folder dintr-un circuit al încrederii decriptează folderul și întregul său conținut, anulând protecția acestora.

- Din modul de vizualizare Trust Circle, efectuați clic pe sau atingeți **Your Trust Circles** (Circuitele dvs. ale încrederii), efectuați dublu clic pe sau atingeți de două ori circuitul existent al încrederii pentru a afișa folderele existente și apoi efectuați clic pe sau atingeți pictograma **coș de gunoi** de lângă respectivul folder.

  – sau –

- În Windows Explorer, efectuați clic dreapta pe sau atingeți și țineți apăsat un folder care face parte la momentul respectiv dintr-un circuit al încrederii, apoi selectați **Trust Circle** și selectați **Remove from trust circle** (Eliminare din circuitul încrederii).

SFAT: Puteți selecta unul sau mai multe foldere.

Eliminarea unui fișier dintr-un circuit al încrederii

Pentru a elimina un fișier dintr-un circuit al încrederii, din Windows Explorer efectuați clic dreapta pe sau atingeți și țineți apăsat un fișier care este criptat la momentul respectiv, selectați **Trust circle** şi selectaţi **Decriptare fişier**.

Eliminarea de membri dintr-un circuit al încrederii

Un membru care a fost înregistrat cu drepturi depline nu poate fi eliminat dintr-un circuit al încrederii. O metodă alternativă ar fi crearea unui nou circuit al încrederii cu toți ceilalți membri, mutarea tuturor fișierelor și folderelor în noul circuit al încrederii și apoi ștergerea vechiului circuit al încrederii. Aceasta vă va oferi certitudinea că orice noi fișiere pe care membrul le primește nu vor fi accesibile, însă tot ceea ce a fost partajat anterior va rămâne accesibil membrului vechiului circuit al încrederii.

Dacă membrul nu este înregistrat cu drepturi depline (fie membrul a fost invitat să se alăture circuitului încrederii, fie nu a acceptat invitația în circuitul încrederii), puteți elimina membrul din circuitul încrederii într-unul din următoarele moduri:

- Din modul de vizualizare Trust Circle, atingeți **Your Trust Circles** (Circuitele dvs. ale încrederii) și apoi efectuați dublu clic pe sau atingeți de două ori circuitul încrederii pentru a fișa lista actuală de membri. Efectuați clic pe sau atingeți pictograma **coș de gunoi** de lângă numele membrului care trebuie eliminat.
- Din modul de vizualizare Trust Circle, efectuați clic pe sau atingeți **Membri** și apoi efectuați dublu clic sau atingeți de două ori membrul pentru a afișa circuitele încrederii de care acesta aparține. Efectuați clic pe sau atingeți pictograma **coș de gunoi** de lângă un circuit al încrederii pentru a elimina membrul din respectivul circuit al încrederii.

Ștergerea unui circuit al încrederii

Pentru a șterge un circuit al încrederii, trebuie să fiți inițiatorul acestuia.

▲ Din modul de vizualizare Trust Circle, efectuați clic pe sau atingeți **Your Trust Circles** (Circuitele dvs. ale încrederii) și efectuați clic pe sau atingeți pictograma **coș de gunoi** de lângă circuitul încrederii care trebuie șters.

Aceasta va șterge circuitul încrederii din pagină și va trimite e-mailuri către toți membrii circuitului încrederii, informându-i cu privire la ștergerea respectivului circuit al încrederii. Orice fișiere sau foldere care au fost incluse în respectivul circuit al încrederii sunt decriptate.

Configurarea preferințelor

Din modul de vizualizare Trust Circle, efectuați clic pe sau atingeți **Preferințe**. Sunt afișate trei file

- **Configurări de e-mail**

Opțiune	Descriere
Nume de utilizator	Este afișat numele de utilizator folosit la momentul respectiv. Pentru a-l schimba, tastați un nou nume de utilizator în caseta text. Modificările sunt salvate automat.
Adresă de e-mail	Se afișează contul de e-mail utilizat la momentul respectiv. Pentru a-l modifica, efectuați clic pe sau atingeți **Change Email Settings** (Modificare configurări de e-mail) și apoi urmați instrucțiunile de pe ecran.
Confirmarea noului membru	Selectați dintre următoarele opțiuni: ◦ **Confirm Automatically** (Confirmare automată)—După primirea acceptului persoanei/persoanelor invitate, acestea sunt confirmate în circuitul încrederii fără alte operațiuni manuale. Persoana/persoanele respective vor primi un e-mail de confirmare. ◦ **Confirm Manually** (Confirmare manuală)—După primirea acceptului persoanei/persoanelor invitate, sunt necesare anumite operațiuni manuale pentru a înregistra noii membri în circuitul încrederii. Apoi, se va trimite un e-mail de confirmare către persoana/persoanele invitate. ◦ **Require verification** (Necesită verificare)—După primirea acceptului de la persoana/persoanele invitate, este necesar un cod de verificare pentru înregistrarea cu drepturi depline a persoanei/persoanelor invitate. Deținătorul circuitului încrederii trebuie să contacteze persoana/persoanele invitate și să primească codul de verificare de la acestea. După tastarea codului corect, se trimit e-mailurile de confirmare.
Autentificare periodică	Autentificarea periodică necesită tastarea de către utilizator a parolei Windows după perioada de expirare specificată (înregistrată în minute) și de asemenea în timpul derulării de operațiuni confidențiale. Această configurare le permite utilizatorilor să pornească sau să oprească autentificarea.
Perioada de expirare a autentificării	Selectați perioada specificată de expirare (înregistrată în minute) înainte de a fi necesară autentificarea.
Nu afișa mesajul de confirmare	Selectați caseta de bifare pentru a dezactiva afișarea mesajelor de confirmare, sau deselectați caseta de bifare pentru a afișa mesajele de confirmare.
Aș dori să ajut la îmbunătățirea aplicației HP Trust Circle prin monitorizarea anonimă a utilizării	Selectați caseta de bifare pentru a participa la acest program sau deselectați-o dacă nu doriți să participați.

- **Copiere de rezervă/Restaurare**

Opțiune	Descriere
Copiere de rezervă	Copiază datele dvs. din aplicația Trust Circle Manager/Reader (configurările și circuitele încrederii) într-un fișier copie de rezervă. În eventualitatea unei avarii sau defecțiuni a sistemului, puteți utiliza acest fișier pentru a vă restaura noua instalare a Trust Circles în starea salvată în fișier. **NOTĂ:** Se salvează numai datele privind aplicația dvs. Trust Circle (circuitele încrederii, configurările și membrii). Fișierele efective din folderele din cadrul circuitului încrederii nu beneficiază de copii de rezervă. Ar trebui să efectuați copii de rezervă separate pentru aceste fișiere. Pentru a face copii de rezervă ale configurărilor Trust Circle și ale datelor utilizatorului: **1.** Efectuați clic pe sau atingeți **Copiere de rezervă**. **2.** Alegeți un nume de fișier și un director pentru fișierul copie de rezervă și apoi efectuați clic pe sau atingeți **Salvare**. **3.** Tastați o parolă, confirmați-o și apoi efectuați clic pe sau atingeți **OK**. Această parolă va fi necesară pentru restaurarea respectivului fișier.
Restaurarea	Restaurează configurările și circuitele încrederii dintr-un fișier copie de rezervă, de obicei după o defecțiune a sistemului sau după o migrare pe un alt computer. Pentru a restaura configurările și datele utilizatorului din Trust Circle Manager: **1.** Efectuați clic pe sau atingeți **Restaurare**. **2.** Navigați la directorul și denumirea fișierului copie de rezervă și apoi efectuați clic pe sau atingeți **Deschidere**. **3.** Tastați parola care a fost configurată în momentul efectuării copiei de rezervă.

- **Despre**—Se afișează informații despre versiunea software-ului Trust Circle Manager/Reader. Se afișează link-uri care vă permit să actualizați Trust Circle Manager la versiunea Pro sau să afișați prevederile HP referitoare la confidențialitate.

9 Theft Recovery (Recuperare furt) (numai la anumite modele)

Computrace (cumpărat separat) vă permite să monitorizaţi, să administraţi la distanţă şi să urmăriţi computerul dvs.

Odată activat, Computrace este configurat din Centrul pentru clienţi Absolute Software. Din Centrul pentru clienţi, administratorul poate configura Computrace pentru a monitoriza sau administra computerul. Dacă sistemul este înlocuit sau furat, Centrul pentru clienţi poate ajuta autorităţile locale la localizarea şi recuperarea computerului. Dacă este configurat, Computrace continuă să funcţioneze chiar dacă unitatea de disc este ştearsă sau înlocuită.

Pentru a activa Computrace:

1. Conectaţi-vă la Internet.
2. Deschideţi HP Client Security. Pentru mai multe informaţii, consultaţi Deschiderea HP Client Security, la pagina 9.
3. Efectuaţi clic pe Theft Recovery **(Recuperare furt)**.
4. Pentru a lansa Expertul de activare Computrace, efectuaţi clic pe **Începeţi**.
5. Introduceţi informaţiile dvs. de contact şi informaţiile de plată cu cardul de credit sau introduceţi o cheie de produs cumpărată în prealabil.

Expertul de activare procesează în mod securizat tranzacţia şi configurează contul dvs. de utilizator pe site-ul Web Centrul pentru clienţi Absolute Software. După finalizare, veţi primi o confirmare prin e-mail ce conţine informaţiile contului dvs. Centrul pentru clienţi.

Dacă aţi executat anterior Expertul de activare Computrace şi contul dvs. de utilizator Centrul pentru clienţi există deja, puteţi să achiziţionaţi licenţe suplimentare, contactând reprezentantul de conturi HP.

Pentru a vă conecta la Centrul pentru clienţi:

1. Accesaţi https://cc.absolute.com/.
2. În câmpurile **ID de conectare** şi **Parolă**, introduceţi acreditările pe care le primiţi în e-mailul de confirmare, apoi efectuaţi clic pe **Conectare**.

Folosind Centrul pentru clienţi, puteţi să:

- Monitorizaţi computerele dvs.
- Protejaţi datele la distanţă.
- Raportaţi furtul oricărui computer protejat de Computrace.

▲ Efectuaţi clic pe **Aflaţi mai multe** pentru mai multe informaţii despre Computrace.

10 Excepții privind parolele localizate

La nivelul autentificării la pornire și la nivelul HP Drive Encryption, asistența pentru localizarea parolelor este limitată. Pentru mai multe informaţii, consultaţi IME-urile Windows nu sunt acceptate la nivelul autentificării la pornire sau la nivelul Drive Encryption., la pagina 55.

Ce trebuie făcut în momentul în care se respinge o parolă

Parolele pot fi respinse din următoarele motive:

- Utilizatorul folosește un IME care nu este acceptat. Aceasta este o problemă des întâlnită în cazul limbilor de doi octeți (coreeană, japoneză, chineză). Pentru a soluționa problema:

  1. Folosind **Panoul de control**, adăugați o configurație acceptată a tastaturii (adăugați tastaturile Engleză SUA din Limbă de intrare chineză).
  2. Configurați tastatura acceptată pentru modul de tastare implicit.
  3. Lansați HP Client Security și apoi tastați parola Windows.

- Utilizatorul folosește un caracter care nu este acceptat. Pentru a soluționa problema:

  1. Modificați parola Windows astfel încât aceasta să conțină numai caractere acceptate. Pentru mai multe informații despre caracterele care nu sunt acceptate, consultați Utilizarea tastelor speciale, la pagina 56.
  2. Lansați HP Client Security și apoi tastați parola Windows.

IME-urile Windows nu sunt acceptate la nivelul autentificării la pornire sau la nivelul Drive Encryption.

În Windows, utilizatorul poate alege un IME (editor metodă de tastare) pentru a tasta caractere și simboluri complexe, precum caractere japoneze sau chineze, folosind o tastatură vestică standard.

IME-urile nu sunt acceptate la nivelul autentificării la pornire sau la nivelul Drive Encryption. Parola Windows nu poate fi tastată cu un IME în momentul autentificării la pornire sau pe ecranul de autentificare HP Drive Encryption, iar în cazul în care aceasta este totuși tastată, va rezulta o blocare. În anumite cazuri, Microsoft® Windows nu afişează IME-ul atunci când utilizatorul tastează parola.

Soluția este să se comute la una dintre configurațiile acceptate ale tastaturii, care traduce în configurația tastaturii 00000411:

- IME Microsoft pentru japoneză
- Configurația tastaturii pentru japoneză
- IME-ul Office 2007 pentru japoneză - Dacă Microsoft sau un terț folosește termenul IME sau editor metodă de tastare, atunci metoda de tastare poate să nu fie de fapt un IME. Aceasta poate genera confuzii, însă software-ul citește reprezentarea codului hexadecimal. Astfel, dacă un IME se mapează pe o configurație acceptată a tastaturii, atunci HP Client Security poate accepta configurația.

⚠ **AVERTISMENT!** Atunci când se implementează HP Client Security, parolele tastate cu un IME Windows vor fi respinse.

Modificarea parolelor folosind configurația tastaturii care este de asemenea acceptată

Dacă parola este configurată inițial folosindu-se o singură configurație a tastaturii, precum Engleză SUA (409) și apoi utilizatorul modifică parola folosind o configurație diferită a tastaturii, care este de asemenea compatibilă, precum cea Latino-americană (080A), modificarea parolei va funcționa în HP Drive Encryption, însă nu va funcționa în BIOS dacă utilizatorul folosește caractere care există în cea de-a doua însă nu și în prima (de exemplu ē).

NOTĂ: Administratorii pot soluționa această problemă folosind pagina Utilizatori HP Client Security (accesată din pictograma **Echipament** din pagina de întâmpinare) pentru a șterge utilizatorul din HP Client Security, selectând configurația dorită a tastaturii din sistemul de operare și apoi rulând expertul de configurare HP Client Security din nou, pentru același utilizator. BIOS stochează configurația dorită a tastaturii, iar parolele care pot fi tastate folosindu-se această configurație a tastaturii vor fi configurate adecvat în BIOS.

O altă problemă potențială este utilizarea unor configurații diferite ale tastaturii care pot produce aceleași caractere. De exemplu, atât configurația SUA internațională (20409), cât și configurația Latino-americană (080A) pot genera caracterul é, deși pot fi necesare combinații de taste diferite. Dacă o parolă este configurată inițial cu configurația Latino-americană a tastaturii, atunci configurația Latino-americană este configurată în BIOS, chiar dacă parola este schimbată ulterior, folosindu-se configurația SUA internațională.

Utilizarea tastelor speciale

- Chineză, slovacă, franceză Canada și cehă

  Atunci când un utilizator selectează una dintre configuraţiile precedente ale tastaturii şi apoi tastează o parolă (de exemplu abcdef), aceeaşi parolă trebuie tastată când se apasă tasta shift pentru minuscule şi tasta shift şi tasta caps lock pentru majuscule în Autentificarea la pornire şi HP Drive Encryption. Parolele numerice trebuie tastate folosindu-se tastatura numerică.

- Coreeană

  Atunci când un utilizator selectează o configuraţie coreeană acceptată a tastaturii şi apoi tastează o parolă, aceeaşi parolă trebuie tastată când se apasă tasta alt din dreapta pentru minuscule şi tasta alt din dreapta şi tasta caps lock pentru majuscule în Autentificarea la pornire şi HP Drive Encryption.

- Caracterele neacceptate sunt indicate în tabelul următor:

Language (Limba)	Windows	BIOS	Drive Encryption
Arabă	Tastele ﻻ ,ﻷ și ﻹ generează două caractere.	Tastele ﻻ ,ﻷ și ﻹ generează un caracter.	Tastele ﻻ ,ﻷ și ﻹ generează un caracter.
Franceză Canada	ç, è, à şi é cu caps lock sunt Ç, È, À şi É în Windows.	ç, è, à şi é cu caps lock sunt ç, è, à şi é în Autentificare la pornire.	ç, è, à şi é cu caps lock sunt ç, è, à şi é în HP Drive Encryption.

Language (Limba)	Windows	BIOS	Drive Encryption
Spaniolă	40a nu este acceptată. Totuși, va funcționa, deoarece software-ul o transformă în c0a. Totuși, din cauza diferențelor subtile dintre configurațiile tastaturii, se recomandă ca vorbitorii de limbă spaniolă să-și schimbe configurația tastaturii Windows în 1040a - Spaniolă (variantă) sau 080a (Latino-americană).	n/a	n/a
SUA internațională	◦ Tastele ¡, ¤, ‘, ’, ¥, și × de pe rândul superior sunt respinse. ◦ Tastele å, ® și Þ de pe cel de-al doilea rând sunt respinse. ◦ Tastele á, ð și ø de pe cel de-al treilea rând sunt respinse. ◦ Tasta æ de pe ultimul rând este respinsă.	n/a	n/a
Cehă	◦ Tasta ğ este respinsă. ◦ Tasta į este respinsă. ◦ Tasta ų este respinsă. ◦ Tastele ė, ı și ż sunt respinse. ◦ Tastele ģ, ķ, ļ, ņ și ţ sunt respinse.	n/a	n/a
Slovacă	Tasta ż este respinsă.	◦ Tastele š, ś și ş sunt respinse atunci când sunt tastate, însă sunt acceptate atunci când sunt tastate folosindu-se tastatura virtuală (soft). ◦ Tasta neutră ţ generează două caractere.	n/a
Maghiară	Tasta ż este respinsă.	Tasta ţ generează două caractere.	n/a
Slovenă	Tasta żŻ este respinsă în Windows, iar tasta alt generează o tastă neutră în BIOS.	Tastele ú, Ú, ů, Ů, ş, Ş, ś, Ś, š și Š sunt respinse în BIOS.	n/a
Japoneză	Atunci când este disponibil, IME-ul Microsoft Office 2007 reprezintă o opțiune mai bună. În ciuda denumirii IME, de fapt configurația 411 a tastaturii este cea acceptată.	n/a	n/a

Glosar

acreditare
O informație specifică sau un dispozitiv hardware folosit pentru autentificarea unui utilizator individual.

activare
Sarcina care trebuie finalizată înainte ca oricare dintre caracteristicile Drive Encryption să devină accesibilă. Administratorii pot activa Drive Encryption cu ajutorul expertului de configurare HP Client Security sau cu ajutorul HP Client Security. Procesul de activare constă din activarea software-ului, din criptarea unității și din crearea cheii de criptare pentru copierea inițială de rezervă pe un dispozitiv de stocare amovibil.

administrator
Consultaţi *Administrator Windows*.

Administrator Windows
Un utilizator cu drepturi depline de a modifica permisiunile și de a gestiona alți utilizatori.

amprentă
Un extras digital al imaginii amprentei dvs. Imagina amprentei dvs. reale nu este stocată niciodată de HP Client Security.

arhivă de recuperare de urgenţă
O zonă de stocare protejată care permite recriptarea cheilor utilizatorului de bază de pe cheia unui proprietar de platformă la alta.

autentificare
Procesul prin care se verifică dacă dvs. sunteți persoana care pretindeți că ați fi, prin folosirea de acreditări, inclusiv a parolei dvs. Windows, a amprentei dvs., a smart cardului, a cardului fără contact sau a cardului de proximitate.

Autentificarea prealabilă încărcării Drive Encryption
Un ecran de conectare care este afișat înainte ca Windows să pornească. Utilizatorii trebuie fie să-și tasteze numele de utilizator Windows și parola, sau PIN-ul smart cardului, sau să efectueze un gest de tragere cu degetul înregistrat. Dacă se selectează conectarea într-o singură etapă, atunci tastarea informațiilor corecte pe ecranul de conectare Drive Encryption va permite un acces direct la Windows fără a fi necesară conectarea din nou prin intermediul ecranului de conectare Windows.

Autentificare JITA (Just in time)
Consultați secțiunea de Ajutor aferentă software-ului HP Device Access Manager.

autentificare la pornire
O caracteristică de securitate care solicită o anumită modalitate de autentificare, precum un smart card, un cip de securitate sau o parolă, atunci când computerul este pornit.

Bluetooth
Tehnologia care folosește transmisiile radio pentru a activa computerele, imprimantele, mouse-urile, telefoanele mobile echipate cu tehnologie Bluetooth, precum și alte dispozitive cu posibilități de comunicație wireless, pe o distanță scurtă.

card de proximitate
Un card din plastic ce conține un cip de computer, care se poate folosi în scopuri de autentificare alături de alte acreditări, pentru o securitate sporită.

card fără contact
Un card din plastic care conține un cip de computer și care se folosește în scopuri de autentificare.

carte de identitate
Un gadget aflat pe desktop-ul Windows care identifică vizual desktopul dvs. cu numele de utilizator şi imaginea aleasă.

Cip embedded security Trusted Platform Module (TPM)
Un TPM autentifică un computer, în loc de un utilizator, prin stocarea de informaţii specifice pentru sistemul gazdă, precum chei de criptare, certificate digitale şi parole. Un TPM minimizează riscul ca informaţiile de pe computer să fie compromise prin furtul fizic sau prin atacul unui hacker extern.

clasă de dispozitive
Toate dispozitivele de un anumit tip, cum ar fi unitățile.

conectare
Un obiect din HP Client Security care este format dintr-un nume de utilizator şi o parolă (şi posibil alte informaţii selectate) care poate fi utilizat pentru a vă conecta la site-urile Web sau alte programe.

cont de reţea
Un cont de utilizator Windows sau de administrator, aflat fie pe un computer local, într-un grup de lucru sau pe un domeniu.

Cont de utilizator Windows
Un utilizator care este autorizat să se conecteze la o rețea sau la un computer individual.

copiere de rezervă
Se folosește caracteristica de copiere de rezervă pentru a salva o copie a informațiilor importante de program, într-un loc din exteriorul programului. Se poate utiliza ulterior pentru restaurarea informațiilor, pe același computer sau pe un computer diferit.

criptare
O procedură, precum utilizarea unui algoritm, folosită în criptografie pentru a converti textul simplu în text cifrat cu scopul de împiedica citirea datelor de către destinatarii neautorizaţi. Există mai multe tipuri de criptare a datelor şi acestea constituie baza de securitate a reţelei. Tipuri comune includ Standardul de criptare a datelor şi criptarea cheie publică.

criptare hardware
Se vor utiliza unitățile cu criptare automată care respectă specificațiile OPAL ale Trusted Computing Group pentru gestionarea unităților cu criptare automată, în vederea executării criptării instantanee. Criptarea hardware este instantanee și poate dura numai câteva minute, însă criptarea software poate dura mai multe ore.

criptare software
Utilizarea unui software pentru criptarea unității de disc, sector cu sector. Acest proces este mai lent decât criptarea hardware

curățarea spațiului liber
Scrierea unor date aleatorii peste elementele șterse și spațiul neutilizat. Acest proces reduce existența elementului șters, astfel încât elementul original este mult mai dificil de recuperat.

decriptare
O procedură utilizată în criptografie pentru a converti datele criptate în text simplu.

dispozitiv conectat
Un dispozitiv hardware care este conectat la un anumit port de pe computer.

distrugere
Executarea unui algoritm care suprascrie peste datele incluse într-un element date fără sens.

distrugere automată
Distrugerea pe care ați programat-o în File Sanitizer.

distrugere manuală

Distrugerea imediată a unui element sau a unor elemente selectate, care nu are legătură cu o distrugere planificată.

domeniu
Un grup de computere care fac parte dintr-o reţea şi partajează o bază de date cu directoare comune. Domeniile sunt denumite individual şi fiecare deţine un set de reguli şi proceduri comune.

Drive Encryption
Protejează datele dvs. prin criptarea unităţilor de disc, asigurându-se că informaţiile nu pot fi citite de către persoanele fără autorizaţia corespunzătoare.

DriveLock
O caracteristică de securitate care face legătura între unitatea de disc şi utilizator şi care solicită acestuia să tasteze corect parola DriveLock în momentul pornirii computerului.

Ecranul de conectare Drive Encryption
A se vedea autentificarea prealabilă încărcării Drive Encryption.

element
O componentă de date care constă din informații sau fișiere personale, date istorice și cele privind navigarea web etc., aflate pe unitatea de disc.

Encryption File System (EFS)
Un sistem care criptează toate fişierele şi subfolderele in cadrul folderului selectat.

Folder Trust Circle
Orice folder protejat de un circuit al încrederii.

grup
Un grup de utilizatori care are același nivel de acces sau refuzare a accesului la o clasă de dispozitive sau la un dispozitiv specific.

identitate
În HP Client Security, un grup de acreditări şi setări care este tratat precum contul sau profilul unui anumit utilizator.

metodă de conectare în siguranţă
Metoda utilizată pentru conectarea la computer.

Pagină principală
Un loc central din care puteți accesa și gestiona caracteristicile și configurațiile din HP Client Security.

PIN
Un număr personal de identificare pentru un utilizator înregistrat, care se folosește în scopuri de autentificare.

PKI
Standardul Public Key Infrastructure (Infrastructură cheie publică) care defineşte interfeţele cu scopul de a crea, utiliza şi administra certificate şi chei criptografice.

politică de control al accesului la dispozitiv
Lista de dispozitive la care utilizatorul beneficiază sau nu de acces.

Recuperare HP SpareKey
Posibilitatea de a vă accesa computerul răspunzând corect la întrebări de securitate.

reiniţializare
Procesul de repornire a computerului.

restaurare
Un proces care copiază informaţiile de program dintr-un fişier copie de rezervă salvat anterior în acest program.

Single Sign On

O funcţie care stochează informaţii de autentificare şi care vă permite să utilizaţi HP Client Security pentru a accesa Internetul şi aplicaţiile Windows care necesită autentificare cu parolă.

smart card
Un dispozitiv hardware care se poate folosi împreună cu un PIN pentru autentificare.

Trust circle
Asigură controlul asupra datelor, prin diseminarea acestora numai către un grup de utilizatori de încredere. Aceasta preîntâmpină accesul accidental sau intenționat la date al persoanelor neautorizate. Securizate cu ajutorul tehnologiei Zero Overhead Key Management de la CryptoMill, datele sunt limitate criptografic la un circuit al încrederii. Aceasta preîntâmpină decriptarea documentelor sau a altor informaţii confidenţiale în afara circuitului încrederii

Trust Circle Manager/Reader
Trust Circle Reader poate accepta numai invitațiile trimise de utilizatorii Trust Circle Manager. Totuși, Trust Circle Manager permite crearea de circuite ale încrederii. Caracteristicile includ invitarea prin e-mail a unei persoane într-un circuit al încrederii și acceptarea invitațiilor transmise de alte persoane într-un circuit al încrederii. Odată ce s-a creat un circuit al încrederii între persoanele implicate, fișierele protejate de respectivul circuit al încrederii pot fi partajate în condiții de siguranță.

utilizator
Orice persoană înregistrată în Drive Encryption. Utilizatorii non-administrator au drepturi limitate în Drive Encryption. Aceştia se pot doar înregistra şi conecta (numai cu aprobarea administratorului).

Windows Logon Security
Protejează contul(urile) dvs. Windows solicitând utilizarea de acreditări specifice pentru acces.

Index