HP Client Security

Първи стъпки

Bluetooth е търговска марка, собственост на своя притежател и използвана от Hewlett-Packard Company с лиценз. Intel е търговска марка на Intel Corporation в САЩ и в други страни и се използва с лиценз. Microsoft и Windows са регистрирани в САЩ търговски марки на Microsoft Corporation.

Информацията, която се съдържа тук, подлежи на промяна без предизвестие. Единствените гаранции за продуктите и услугите на HP са изрично изложени в гаранционните карти, придружаващи въпросните продукти и услуги. Нищо от споменатото тук не следва да се тълкува и приема като допълнителна гаранция. HP не носи отговорност за технически или редакторски грешки или пропуски в настоящия документ.

Първо издание: август 2013 г.

Номенклатурен номер на документа: 735339-261

Съдържание

1 Въведение в HP Client Security Manager

HP Client Security ви дава възможност да защитите данните, устройството и самоличността си, като по този начин подобрява защитата на вашия компютър.

Софтуерните модули, налични за вашия компютър, може да варират в зависимост от модела.

Софтуерните модули на HP Client Security може да бъдат предварително инсталирани, предварително изтеглени или налични за изтегляне от уебсайта на HP. За повече информация вж. http://www.hp.com.

ЗАБЕЛЕЖКА: Инструкциите в настоящото ръководство са написани с презумпцията, че вие вече имате инсталирани приложими софтуерни модули на HP Client Security.

Функции на HP Client Security

Таблицата по-долу изброява основните функции на модулите на HP Client Security.

Модул	Основни функции
HP Client Security Manager	Администраторите могат да извършват следните функции: • Да защитят вашия компютър преди стартирането на Windows® • Да защитят вашия акаунт на Windows с помощта на строго удостоверяване • Да управляват вашите влизания и пароли за уебсайтове и приложения • Да променят лесно вашата парола за операционна система Windows • Да използват пръстови отпечатъци за допълнителна защита и удобство • Да използват смарт карта, безконтактна карта или карта с чип за удостоверяване • Да използват вашия телефон с Bluetooth като метод за идентификация • Да задават PIN код за разширяване на вашите опции за удостоверяване • Да конфигурират правилата за влизане и правилата за сесия • Да архивират и възстановяват вашите програмни данни • Да добавят допълнителни приложения, като например HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager и HP Computrace Обикновените потребители могат да извършват следните функции: • Да разглеждат настройките за състояние на шифроването и Device Access Manager. • Да активират Computrace. • Да конфигурират опциите за предпочитания и опциите за архивиране и възстановяване.
Password Manager	Обикновените потребители могат да извършват следните функции: • Да организират и създават потребителски имена и пароли. • Да създават по-силни пароли за подобрена защита на имейл и уеб акаунтите. Password Manager попълва и изпраща информацията автоматично. • Да опростява процеса на влизане с помощта на функцията за еднократна идентификация, която автоматично запаметява и използва идентификационните данни на потребителя. • Да маркира даден акаунт като компрометиран, за да можете да получавате предупреждения за друг(и) акаунт(и) с подобни идентификационни данни. • Да импортира данните за вход от поддържан браузър.

Модул	Основни функции
HP Drive Encryption (само при определени модели)	• Осигурява пълно и цялостно шифроване на твърдия диск. • Извършва принудително предстартово удостоверяване, за да дешифрира и осъществи достъп до данните. • Предлага опция за активиране на самокодиращи устройства (само при някои модели).
HP Device Access Manager	• Позволява на ИТ мениджърите да контролират достъпа до устройствата на базата на потребителските профили. • Не допуска неупълномощени потребители да прехвърлят данни с помощта на външни носители за съхранение на данни, както и да въвеждат вируси в системата посредством външни носители. • Позволява на администраторите да деактивират достъпа на определени лица или групи потребители до комуникационните устройства.
HP Trust Circles	• Осигурява защита на файловете и документите. • Шифрова файлове, поставени в определени от потребителя папки, и ги защитава в рамките на даден trust circle. • Позволява използване и споделяне на файловете само от членовете на съответния trust circle.
Възстановяване след кражба (Computrace, закупува се отделно)	• Изисква отделно закупуване на абонаменти за прихващане и проследяване, за да се активира. • Осигурява безопасно проследяване на вещи. • Следи активността на потребителите, както и хардуерни и софтуерни промени. • Остава активен, дори след като твърдият диск е преформатиран или сменен.

Описание на продукта HP Client Security и примери за обичайна употреба

Повечето от продуктите на HP Client Security имат функции както за удостоверяване на потребителя (обикновено парола), така и за административно архивиране за осъществяване на достъп, ако паролите се изгубят, не са налични или се забравят, или винаги, когато служителите по корпоративна защита изискат достъп.

ЗАБЕЛЕЖКА: Някои от продуктите на HP Client Security са предназначени да ограничават достъпа до данни. Данните трябва да са шифровани, когато важността им е толкова голяма, че потребителят по-скоро би предпочел да загуби информацията, отколкото да я остави да бъде компрометирана. Препоръчва се всички данни да се архивират на сигурно място.

Password Manager

Password Manager съхранява потребителски имена и пароли и може да се използва за следното:

- Да запазва имена за влизане и пароли за достъп до Интернет или имейл.
- Автоматично да дава достъп на потребителя до даден уебсайт или имейл.

- Да управлява и организира удостоверяванията.
- Да избира уеб или мрежов актив и да осъществява директен достъп до връзката.
- Да показва имена и пароли, когато е необходимо.
- Да маркира даден акаунт като компрометиран, за да можете да получавате предупреждения за друг(и) акаунт(и) с подобни идентификационни данни.
- Да импортира данните за вход от поддържан браузър.

Пример 1: Търговски представител по закупуване на стоки, работещ за голям производител, извършва повечето от своите корпоративни транзакции по Интернет. Тя също така често посещава популярни уебсайтове, които изискват информация за вход. Тя е добре запозната със съображенията за защита и не използва една и съща парола за всеки акаунт. Търговският представител по закупуване на стоки решава да използва Password Manager, за да свърже различни уеб връзки с потребителски имена и пароли. Когато тя влиза в даден уебсайт, Password Manager автоматично въвежда идентификационните данни. Ако тя иска да види потребителските имена и паролите, Password Manager може да бъде конфигуриран така, че да ги показва.

Password Manager може също така да се използва за управление и организиране на удостоверяванията. Този инструмент позволява да даден потребител да избере уеб или мрежов актив и и да осъществи директен достъп до връзката. Потребителят също така може да види потребителските имена и паролите, когато е необходимо.

Пример 2: Трудолюбив служител е повишен и вече ще управлява целия счетоводен отдел. Екипът трябва да влиза в голям брой клиентски уеб акаунти, за всеки от които има различна информация за вход. Тази информация за вход трябва да се споделя с други служители, така че поверителността представлява проблем. Въпросният служител решава да организира всички уеб връзки, потребителски имена на компанията и пароли посредством Password Manager. След като приключва, служителят предоставя на служителите Password Manager, така че те да могат да работят в уеб акаунтите без действително да знаят идентификационните данни за влизане, които използват.

HP Drive Encryption (само при определени модели)

HP Drive Encryption се използва за ограничаване на достъпа до данните на целия твърд диск на компютъра или на допълнително дисково устройство. Drive Encryption може също така да управлява самокодиращи устройства.

Пример 1: Лекар иска да бъде сигурен, че само той ще има достъп до данните на твърдия диск на неговия компютър. Лекарят активира Drive Encryption, което изисква принудително предстартово удостоверяване преди влизане в Windows. След конфигуриране, достъп до твърдия диск не може да бъде осъществен без парола преди стартиране на операционната система. Лекарят може да подобри защитата на диска още повече, като реши да шифрова данните с опцията за самокодиращи устройства.

Пример 2: Болничен администратор иска да бъде сигурен, че само лекари и упълномощени служители могат да осъществяват достъп до данните на локалния компютър без да се налага да споделят личните си пароли. ИТ отделът добавя администратора, лекарите и всички упълномощени служители като потребители на Drive Encryption. Сега само упълномощените служители могат да стартират компютъра или домейна, като използват своите лични потребителски имена и пароли.

HP Device Access Manager (само за избрани модели)

HP Device Access Manager позволява на администратора да ограничава и управлява достъпа до хардуера. Device Access Manager може да се използва за блокиране на неупълномощен достъп до USB устройства, от които данните могат да бъдат копирани. Той също така може да ограничи достъпа до CD/DVD устройства, да контролира USB устройства, мрежови връзки и т.н. Като пример може да бъде дадена ситуация, при която външни доставчици се нуждаят от достъп до фирмените компютри, но не трябва да могат да копират данните на USB устройство.

Пример 1: Управител на фирма за медицински консумативи често работи с лична медицинска документация, както и с информация за фирмата си. Служителите му се нуждаят от достъп до тези данни, но е изключително важно данните да не се пренасят от компютъра чрез USB устройство или друг външен носител. Мрежата е сигурна, но компютрите имат записващи дискови устройства и USB портове, които биха могли да позволят данните да бъдат копирани или откраднати. Управителят използва Device Access Manager , за да блокира USB портовете и записващите дискови устройства, така че те да не могат да се използват. Дори при блокирани USB портове, мишките и клавиатурите ще могат да продължат да функционират.

Пример 2: Застрахователна компания не желае служителите й да инсталират или качват личен софтуер или данни от къщи. Някои служители се нуждаят от достъп до USB портовете на всички компютри. ИТ мениджърът използва Device Access Manager, за да разреши достъпа на някои служители, като същевременно блокира достъпа на външни лица.

Computrace (закупува се отделно)

Computrace (закупува се отделно) е услуга, която може да проследи местоположението на откраднат компютър, когато потребителят влезе в Интернет. Computrace може също така да помогне за дистанционно управление и откриване на местоположението на компютри, както и за наблюдение на на използването на даден компютър и неговите приложения.

Пример 1: Директор на училище инструктира ИТ отдела да следи всички компютри в училището. След като прави инвентаризация на компютрите, ИТ администраторът регистрира всички компютри с Computrace, така че да могат да бъдат проследени, в случай че някога бъдат откраднати. Неотдавна, училището откри, че няколко компютъра липсват и ИТ администраторът уведоми властите и управителите на Computrace. Компютрите бяха открити и върнати на училището от властите.

Пример 2: Фирма за недвижими имоти трябва да управлява и актуализира компютри в цял свят. Фирмата използва Computrace, за да наблюдава и актуализира компютрите без да се налага да изпраща ИТ служител за всеки компютър.

Постигане на ключови цели, свързани със защитата

Модулите на HP Client Security могат да работят заедно, за да предоставят решения за различни проблеми, свързани със защитата, включително следните ключови цели, свързани със защитата:

- Защита срещу планирана кражба
- Ограничаване на достъпа до поверителни данни
- Предотвратяване на неупълномощен достъп от вътрешни или външни места
- Създаване на политики за надеждни пароли

Защита срещу планирана кражба

Като пример за планирана кражба може да се посочи кражбата на компютър с поверителна информация и информация за клиенти на контролно-пропускателен пункт на летище. Следните функции спомагат за защитата срещу планирана кражба:

- Ако е активирана, функцията за принудително предстартово удостоверяване, спомага за предотвратяване на достъпа до операционната система.
  - HP Client Security—Вижте HP Client Security на страница 13.
  - HP Drive Encryption—Вижте HP Drive Encryption (само при определени модели) на страница 32.
- Шифроването помага да се гарантира, че достъп до данните не може да се осъществи, дори ако твърдият диск се извади и инсталира в незащитена система.
- Computrace може да проследи местоположението на компютъра след кражба.
  - Computrace—Вижте Възстановяване след кражба (само при някои модели) на страница 57.

Ограничаване на достъпа до поверителни данни

Представете си, че одитор работи на място във вашата фирма и му е предоставен достъп до компютър, за да извърши проверка на поверителни финансови данни. Вие няма да искате одиторът да може да разпечатва файлове или да ги запазва на устройство за запис, като например компактдиск. Следната функция помага за ограничаване на достъпа до данни:

- HP Device Access Manager позволява на ИТ мениджърите да ограничат достъпа до комуникационните устройства, така че поверителната информация да не може да бъде копирана от твърдия диск. Вижте Системен изглед на страница 46.

Предотвратяване на неупълномощен достъп от вътрешни или външни места

Неупълномощеният достъп до незащитен фирмен компютър представлява много реален риск за корпоративните мрежови ресурси, като например информация от финансовите служби, от изпълнителен директор или от екипа по научни изследвания и развойна дейност, както и информация като документация на пациенти или лична финансова документация. Следните функции помагат за предотвратяване на неупълномощения достъп:

- Ако е активирана, функцията за принудително предстартово удостоверяване, спомага за предотвратяване на достъпа до операционната система. (вижте HP Drive Encryption (само при определени модели) на страница 32.
- HP Client Security помага да се гарантира, че даден неупълномощен потребител не може да вземе паролите или да получи достъп до приложения, защитени с пароли. Вижте HP Client Security на страница 13.
- HP Device Access Manager позволява на ИТ мениджърите да ограничат достъпа до устройствата за запис, така че поверителната информация да не може да бъде копирана от твърдия диск. Вижте HP Device Access Manager (само за избрани модели) на страница 45.

Създаване на политики за надеждни пароли

Ако определена фирмена политика влезе в сила и изисква използването на политика за надеждни пароли за десетки уеб-базирани приложения и бази данни, Password Manager

осигурява защитено хранилище за пароли и удобство за еднократна идентификация. Вижте Password Manager на страница 19.

Допълнителни елементи за защита

Задаване на права за достъп

При управлението на компютърната защита (особено в големи организации), важна практика е да се разделят отговорностите и правата сред различните видове администратори и потребители.

ЗАБЕЛЕЖКА: В малка организация или при лична употреба тези права могат да принадлежат само на един човек.

При HP Client Security отговорностите и правата, свързани със защитата, могат да се разделят на следните права:

- Служител по защитата—Определя нивото на защита на фирмата или мрежата и определя функциите за защита, които да се използват, като например Drive Encryption.

  ЗАБЕЛЕЖКА: Много от функциите на HP Client Security могат да се персонализират от служителя по защитата в сътрудничество с HP. За повече информация вж. http://www.hp.com.

- ИТ администратор—прилага и управлява функциите за защита, определени от служителя по защитата. Може също така да активира и деактивира някои функции. Например, ако служителят по защитата реши да използва смарт карти, ИТ администраторът може да активира режим за използване както на парола, така и на смарт карта.

- Потребител—Използва функциите за защита. Например, ако служителят по защитата и ИТ администраторът са разрешили използването на смарт карти за системата, потребителят може да зададе PIN код за смарт картата и да използва картата за удостоверяване.

ВНИМАНИЕ: Препоръчва се администраторите да следват „най-добрите практики“ при ограничаване на правата на крайните потребители и при ограничаване на потребителския достъп.

Неупълномощените потребители не трябва да получават административни права.

Управление на паролите на HP Client Security

Повечето от функциите на HP Client Security са защитени с пароли. Таблицата по-долу показва най-често използваните пароли, софтуерния модул, където се задава паролата, и функцията на паролата.

Паролите, които се задават и използват само от ИТ администраторите, също са посочени в тази таблица. Всички други пароли могат да се задават от обикновени потребители или администратори.

Парола за HP Client Security	Зададена в следния модул	Функция
Парола за вход в Windows	Контролен панел на Windows или HP Client Security	Може да се използва за ръчно влизане и за удостоверяване за достъп до различни функции на HP Client Security.

Парола за HP Client Security	Зададена в следния модул	Функция
Парола за архивиране и възстановяване на HP Client Security	HP Client Security, от отделен потребител	Защитава достъпа до файла за архивиране и възстановяване на HP Client Security.
PIN код за смарт карта	Credential Manager	Може да се използва като многофакторно удостоверяване. Може да се използва като удостоверяване за Windows. Удостоверява потребители на Drive Encryption, ако е избрана смарт картата.

Създаване на защитена парола

При създаване на пароли трябва първо да следвате спецификациите, зададени от програмата. Като цяло, обаче, вземете предвид следните указания, които ще ви помогнат да създадете надеждни пароли и да намалите вероятността за тяхното компрометиране:

- Използвайте пароли с повече от 6 (за предпочитане е повече от 8) символа.
- Използвайте както малки, така и главни букви в паролата си.
- Когато е възможно, използвайте букви и цифри и включете специални символи и препинателни знаци.
- Заменете буквите със специални символи или цифри в дадена ключова дума. Например, можете да използвате цифрата 1 вместо буквите I или L.
- Комбинирайте думи от 2 или повече езика.
- Разделете дума или фраза с цифри или специални символи по средата, например: „Mary2-2Cat45“.
- Не използвайте парола, която би могла да се открие в речник.
- Не използвайте името си или друг тип лична информация, като например вашата дата на раждане, имена на домашни любимци, или моминското име на майка ви, дори ако го напишете в отзад напред.
- Сменяйте паролите си редовно. Можете да сменяте само по няколко символа.
- Ако запишете паролата си, не я съхранявайте на видно място, което е в непосредствена близост до компютъра.
- Не запазвайте паролата си във файл, било то в имейл или в компютъра.
- Не споделяйте акаунти и не казвайте паролата си на никого.

Архивиране на идентификационни данни и настройки

Можете да използвате инструмента за архивиране и възстановяване в HP Client Security като централно място, от което можете да архивирате и възстановявате идентификационни данни за защита от някои от инсталираните модули на HP Client Security.

2 Първи стъпки

За да конфигурирате HP Client Security за използване с вашите идентификационни данни, стартирайте HP Client Security по един от следните начини. Веднъж след като съветникът бъде използван от даден потребител, той не може да се стартира отново от същия потребител.

1. От стартовия екран или екран Приложения, щракнете или натиснете приложението **HP Client Security** (Windows 8).

   – или –

   От работния плот на Windows щракнете или натиснете притурката **HP Client Security** (Windows 7).

   – или –

   От работния плот на Windows щракнете двукратно или натиснете двукратно иконата **HP Client Security** в областта за уведомяване, разположена най-вдясно на лентата със задачи.

   – или –

   От работния плот на Windows щракнете двукратно върху иконата **HP Client Security** в областта за уведомяване, после изберете **Отваряне на HP Client Security**.

2. Съветникът за конфигуриране на HP Client Security се стартира и се показва страницата "Добре дошли".

3. Прочетете екрана "Добре дошли", потвърдете вашата самоличност, като въведете паролата си за Windows, после щракнете или натиснете **Next** (Напред).

   Ако все още не сте създали парола за Windows, ще бъдете подканени да създадете такава. Паролата за Windows се изисква с цел защита на вашия акаунт в Windows от непозволен достъп и с цел използване на функциите на HP Client Security.

4. На страницата HP SpareKey изберете три въпроса за защита. Въведете отговор на всеки въпрос и щракнете върху **Next** (Напред). Позволени са и персонализирани въпроси. За повече информация вж. HP SpareKey—Възстановяване на парола на страница 15.

5. На страницата Пръстови отпечатъци регистрирайте поне минималния брой пръстови отпечатъци, после щракнете или натиснете **Next** (Напред). За повече информация вж. Пръстови отпечатъци на страница 14.

6. На страницата Drive Encryption активирайте шифроването, архивирайте ключа за шифроване, после щракнете или натиснете **Next** (Напред). За повече информация вижте Помощ в софтуера HP Drive Encryption.

ЗАБЕЛЕЖКА: Това се отнася за случая, в който потребителят е администратор и съветникът за конфигуриране на HP Client Security не е конфигуриран от администратор преди това.

7. На последната страница на съветника щракнете или натиснете **Finish** (Край).

   Тази страница предоставя състоянието на функциите и идентификационните данни.

8. Съветникът за конфигуриране на HP Client Security осигурява активирането на функциите Just In Time Authentication и File Sanitizer. За повече информация вижте Помощ в софтуера HP Device Access Manager и HP File Sanitizer.

ЗАБЕЛЕЖКА: Това се отнася за случая, в който потребителят е администратор и съветникът за конфигуриране на HP Client Security не е конфигуриран от администратор преди това.

Отваряне на HP Client Security

Можете да отворите приложението HP Client Security по един от следните начини:

ЗАБЕЛЕЖКА: Съветникът за конфигуриране на HP Client Security трябва да е приключил, преди да можете да стартирате приложението HP Client Security.

- От стартовия екран или екран Приложения, щракнете или натиснете приложението **HP Client Security**.

  – или –

  От работния плот на Windows щракнете или натиснете притурката **HP Client Security** (Windows 7).

  – или –

  От работния плот на Windows щракнете двукратно или натиснете двукратно иконата **HP Client Security** в областта за уведомяване, разположена най-вдясно на лентата със задачи.

  – или –

  От работния плот на Windows щракнете двукратно върху иконата **HP Client Security** в областта за уведомяване, после изберете **Отваряне на HP Client Security**.

3 Ръководство за лесно конфигуриране за малка фирма

Тази глава има за цел да покаже основните стъпки за активиране на най-често срещаните и полезни опции в HP Client Security за малка фирма. Многобройните инструменти и опции в този софтуер ви позволяват да направите фина настройка на вашите предпочитания и да зададете контрол на достъпа. Целта на това Ръководство за лесно конфигуриране е да направи така, че всеки модул да може да работи с минимални усилия и време за конфигуриране. За допълнителна информация, изберете модула, от който се интересувате, а след това щракнете върху **?** или бутона „Помощ“ в горния десен ъгъл. Този бутон автоматично ще покаже информация, която ще ви помогне за текущия прозорец.

Първи стъпки

1. От работния плот на Windows отворете HP Client Security, като щракнете двукратно върху иконата **HP Client Security** в областта за уведомяване, разположена най-вдясно на лентата със задачи.
2. Въведете вашата парола за Windows или създайте парола за Windows.
3. Завършете конфигурирането на HP Client Security.

Ако желаете HP Client Security да изисква удостоверяване само веднъж по време на влизане в Windows, вижте Функции за защита на страница 28.

Password Manager

Всеки разполага с няколко пароли – особено ако редовно влиза в уебсайтове или използва приложения, които изискват влизане. Нормалният потребител или използва една и съща парола за всяко приложение и уебсайт, или става креативен и бързо забравя коя парола за кое приложение се отнася.

Password Manager може автоматично да запомни паролите ви или да ви даде възможността да разпознавате кои сайтове да помните и кои да пропускате. След като влезете в компютъра, Password Manager ще ви предостави вашите пароли или идентификационни данни за участващите приложения или уебсайтове.

Когато влезете в приложение или уебсайт, който изисква идентификационни данни, Password Manager автоматично ще разпознае сайта и ще ви попита дали желаете софтуерът да запомни вашата информация. Ако желаете да изключите определени сайтове, можете да отклоните поканата.

За да започнете да запазвате уеб локации, потребителски имена и пароли:

1. Например, отидете в участващ уебсайт или приложение и щракнете върху иконата на Password Manager в горния ляв ъгъл на уебстраницата, за да добавите уеб удостоверяването.
2. Дайте име на връзката (по избор) и въведете потребителско име и парола в Password Manager.

3. Когато сте готови, щракнете върху бутона **OK** .
4. Password Manager може също така да запази вашето потребителско име и пароли за мрежови ресурси или изобразени мрежови устройства.

Преглед и управление на удостоверяванията в Password Manager

Password Manager ви позволява да разглеждате, управлявате, архивирате и стартирате вашите удостоверявания от централно място. Password Manager също така поддържа стартирането на запазени сайтове от Windows.

Използвайте комбинацията от клавиши на клавиатурата Ctrl+клавиш Windows+h , за да отворите Password Manager, а след това щракнете върху **Log in** , за да стартирате и удостоверите запазения пряк път.

Опцията **Редактиране** на Password Manager ви позволява да разгледате и промените името за влизане, а също така да разкриете паролите.

HP Client Security за малка фирма позволява всички идентификационни данни и настройки да се архивират и/или копират на друг компютър.

HP Device Access Manager

Device Access Manager може да се използва за ограничаване на употребата на различни вътрешни и външни устройства за съхранение, така че вашите данни да останат защитени на твърдия диск и да не напуснат офиса на фирмата ви. Като пример може да бъде даден случай, при който вие давате на потребител достъп до данните, но ограничавате възможността той да ги копира на компактдиск, личен музикален плейър или USB запаметяващо устройство.

1. Отворете **Device Access Manager** (вижте Отваряне на Device Access Manager на страница 46).

   Показан е достъпът за текущия потребител.
2. За да промените достъпа за потребители, групи или устройства, щракнете или натиснете **Change** (Смяна). За повече информация вж. Системен изглед на страница 46.

HP Drive Encryption

HP Drive Encryption се използва за защита на вашите данни чрез шифроване на целия твърд диск. Данните на вашия твърд диск ще останат защитени, дори ако компютърът ви бъде откраднат и/или ако твърдият диск бъде изваден от оригиналния компютър и поставен в друг компютър.

Допълнително предимство по отношение на защитата е, че Drive Encryption изисква от вас правилно удостоверяване с използване на вашето потребителско име и парола преди стартиране на операционната система. Този процес се нарича принудително предстартово удостоверяване.

За ваше улеснение, многобройни софтуерни модули синхронизират паролите автоматично, включително потребителските акаунти в Windows, домейните за удостоверяване, HP Drive Encryption, Password Manager и HP Client Security.

За да конфигурирате HP Drive Encryption по време на първоначалното конфигуриране със съветника за HP Client Security, вижте Първи стъпки на страница 9.

4 HP Client Security

Началната страница на HP Client Security е централното място за лесен достъп до функциите, приложенията и настройките в HP Client Security. Началната страница е разделена на три секции:

- **ДАННИ**—Предоставя достъп до приложения, използвани за управление на защитата на данните.
- **УСТРОЙСТВО**—Предоставя достъп до приложения, използвани за управление на защитата на устройствата.
- **САМОЛИЧНОСТ**—Предоставя регистрация и управление на идентификационни данни за удостоверяване.

Движете курсора над плочката на приложението, за да се покаже описанието на приложението.

HP Client Security може да предостави връзки към потребителски и административни настройки в долната част на страницата. HP Client Security предоставя достъп до разширени настройки и функции чрез натискане или щракване върху иконата **Gear** (настройки).

Функции за идентификация, приложения и настройки

Функциите за идентификация, приложения и настройки, предоставяни от HP Client Security ви помагат в управлението на различни аспекти от вашата цифрова самоличност. Щракнете или натиснете някоя от следните плочки на началната страница на HP Client Security и въведете вашата парола за Windows:

- **Пръстови отпечатъци**—Регистрира и управлява вашите пръстови отпечатъци за идентификация.
- **SpareKey**—Конфигурира и управлява вашите идентификационни данни за HP SpareKey, които могат да се използват за влизане в компютъра, ако сте загубили другите си идентификационни данни. Позволява ви също да промените забравена парола.
- **Парола за Windows**—Предоставя лесен достъп за смяна на паролата за Windows.
- **Bluetooth устройства**—Позволява ви да регистрирате и управлявате вашите Bluetooth устройства.
- **Карти**—Позволява ви да регистрирате и управлявате вашите смарт карти, безконтактни карти и карти с чипове.
- **PIN**—Позволява ви да регистрирате и управлявате вашата идентификация с PIN код.
- **RSA SecurID**—Позволява ви да регистрирате и управлявате вашата RSA SecurID идентификация (ако е извършено правилно конфигуриране).
- **Password Manager**—Позволява ви да управлявате паролите за вашите онлайн акаунти и приложения.

Пръстови отпечатъци

Съветникът за конфигуриране на HP Client Security ви води през процеса на настройка или “ регистриране” на вашите пръстови отпечатъци.

Можете също да регистрирате или изтриете вашите пръстови отпечатъци от страницата Пръстови отпечатъци, която можете да отворите, като щракнете или натиснете иконата **Fingerprints** (Пръстови отпечатъци) в началната страница на HP Client Security.

1. На страницата Пръстови отпечатъци плъзнете пръста си, докато го регистрирате успешно.

   Броят на пръстите, които трябва да бъдат регистрирани, е указан на страницата. За предпочитане са показалец или среден пръст.

2. За да изтриете регистрираните преди това пръстови отпечатъци, щракнете или натиснете **Delete** (Изтриване).

3. За да регистрирате допълнителни пръстови отпечатъци, щракнете или натиснете **Регистриране на допълнителен пръст**.

4. Щракнете или натиснете **Save** (Запис), преди да напуснете страницата.

⚠ **ВНИМАНИЕ:** Когато регистрирате пръстови отпечатъци през съветника, информацията за пръстовия отпечатък не се записва, докато не натиснете **Next** (Напред). Ако оставите компютъра неактивен за известно време или затворите програмата, промените, които сте направили, **няма** да бъдат записани.

- ▲ За достъп до Административни настройки за пръстови отпечатъци, където администраторите могат да зададат регистрирането, точността и други настройки, щракнете или натиснете **Administrative Settings** (Административни настройки)(изисква административни права).
- ▲ За достъп до Потребителски настройки за пръстови отпечатъци, където можете да укажете настройките, които управляват изгледа и поведението при разпознаване на пръстов отпечатък, щракнете или натиснете **User Settings** (Потребителски настройки).

Административни настройки за пръстови отпечатъци

Администраторите могат да зададат регистрация, точност и други настройки на четеца на пръстови отпечатъци. Изискват се административни права.

- ▲ За достъп до Административни настройки за пръстови отпечатъци, щракнете или натиснете **Administrative Settings** (Административни настройки) на страницата Пръстови отпечатъци.

- **Регистриране на потребител**—Изберете минималния и максималния брой пръстови отпечатъци, които потребителят може да регистрира.
- **Разпознаване**—Преместете плъзгача, за да конфигурирате чувствителността, използвана от четеца на пръстови отпечатъци при плъзгане на пръста.

  Ако вашият пръстов отпечатък не се разпознава всеки път, можете да изберете по-ниска настройка за разпознаване. По-високата настройка увеличава чувствителността спрямо промени в плъзгането на пръстовия отпечатък и следователно намалява възможността за фалшиво приемане. Настройката **Средно висока** предоставя добра комбинация от защита и удобство.

Потребителски настройки за пръстови отпечатъци

От страницата Потребителски настройки за пръстови отпечатъци можете да зададете настройките, които управляват изгледа и поведението при разпознаване на пръстов отпечатък.

▲ За достъп до Потребителски настройки за пръстови отпечатъци, щракнете или натиснете **User Settings** (Потребителски настройки) на страницата Пръстови отпечатъци.

- **Разрешаване на звукова информация**—По подразбиране HP Client Security предоставя звукова информация при плъзгане на пръстов отпечатък, като възпроизвежда различни звукове при конкретни събития в програмата. Можете да назначите нови звукове за тези събития през раздела Звуци в настройката на звука в контролния панел на Windows или да забраните звуковата информация, като махнете отметката.
- **Показване на информация за качество на сканирането**—За да се покажат всички плъзгания независимо от качеството, изберете отметката. Махнете отметката, за да се показват само плъзганията с добро качество.

HP SpareKey—Възстановяване на парола

HP SpareKey ви позволява да получите достъп до вашия компютър (на поддържани платформи), като отговорите на три въпроса за защита.

HP Client Security ви подканя да настроите ваш личен HP SpareKey по време на началната настройка в Съветника за конфигуриране на HP Client Security.

За да конфигурирате вашия HP SpareKey:

1. От страницата HP SpareKey в съветника изберете три въпроса за защита, а после отговорете на всеки от тях.

   Можете да изберете въпрос от предварително дефиниран списък или да напишете ваши собствени въпроси.

2. Щракнете или натиснете **Enroll** (Регистрация).

За да изтриете вашия HP SpareKey:

▲ Щракнете или натиснете **Delete your SpareKey** (Изтриване на вашия SpareKey).

След като SpareKey е конфигуриран, можете да получите достъп до компютъра, като използвате SpareKey от екрана за влизане Удостоверяване при включване или от приветстващия екран на Windows.

Можете да изберете различни въпроси или да промените отговорите си на страницата SpareKey, която можете да отворите от плочката Възстановяване на парола от началната страница на HP Client Security.

За достъп до Настройки на HP SpareKey, където администраторът може да зададе настройки, свързани с идентификационни данни за HP SpareKey, щракнете върху **Settings** (Настройки) (изисква административни права).

Настройки на HP SpareKey

От страницата Настройки на HP SpareKey можете да зададете настройките, които управляват поведението и използването на идентификационните данни за HP SpareKey.

▲ За да стартирате страницата Настройки на HP SpareKey, щракнете или натиснете **Settings** (Настройки) на страницата HP SpareKey (изисква административни права).

Администраторите могат да изберат следните настройки:

- Задайте въпросите, които ще бъдат предоставени на всеки потребител при конфигуриране на HP SpareKey.
- Добавете до три персонализирани въпроса за защита, които ще добавите към списъка за потребителите.
- Изберете дали ще позволите или не на потребителите да създават техни собствени въпроси за защита.
- Задайте коя среда за удостоверяване (Windows или Удостоверяване при включване) ще позволи използването на HP SpareKey за възстановяване на паролата.

Парола за Windows

С HP Client Security смяната на паролата за Windows е по-лесно и по-бързо, отколкото през контролния панел на Windows.

За да смените вашата парола за Windows:

1. От началната страница на HP Client Security щракнете или натиснете **Windows Password** (Парола за Windows).
2. Въведете вашата текуща парола в полето **Текуща парола за Windows**.
3. Въведете новата парола в полето **Нова Windows парола**, после я въведете отново в полето **Потвърждаване на новата парола**.
4. Щракнете или натиснете **Change** (Смяна), за да смените веднага вашата текуща парола с новата, която сте въвели.

Bluetooth устройства

Ако администраторът е разрешил Bluetooth като начин за въвеждане на идентификационни данни за удостоверяване, можете да конфигурирате Bluetooth телефон в комбинация с други идентификационни данни за допълнителна защита.

ЗАБЕЛЕЖКА: Поддържат се само Bluetooth телефони.

1. Уверете се, че Bluetooth функционалността е разрешена на компютъра, и че Bluetooth телефонът е настроен в режим на търсене. За да свържете телефона, може да се изисква да въведете автоматично генерирания код на Bluetooth устройството. В зависимост от конфигурационните настройки на Bluetooth устройството, може да се изисква сравнение на кодовете за сдвояване между компютъра и телефона.
2. За да регистрирате телефон, изберете го, после щракнете или натиснете **Enroll** (Регистрация).

За достъп до страницата Настройки на Bluetooth устройства на страница 16, където администраторът може да зададе настройките за Bluetooth устройствата, щракнете върху **Settings** (Настройки) (изисква административни права).

Настройки на Bluetooth устройства

Администраторите могат да зададат настройките, които управляват поведението и използването на идентификационните данни за Bluetooth устройства:

Негласно удостоверяване

- **Автоматично използване на вашето свързано регистрирано Bluetooth устройство по време на проверка на вашата самоличност**—Изберете отметката, за да разрешите на потребителите да използват идентификационни данни от Bluetooth за удостоверяване без намеса на потребител, или махнете отметката, за да забраните тази опция.

Близост на Bluetooth

- **Заключете компютъра, когато вашето регистрирано Bluetooth устройство излезе от обхвата на вашия компютър** —Изберете полето за отметки, за да заключите компютъра, когато дадено Bluetooth устройство, което е било свързано по време на влизане, излезе от обхвата или махнете отметката, за да забраните тази опция.

ЗАБЕЛЕЖКА: Bluetooth модулът на вашия компютър трябва да поддържа тази възможност, за да можете да използвате функцията.

Карти

HP Client Security може да поддържа много различни видове карти за идентификация, които представляват малки пластмасови карти, съдържащи компютърен чип. Те включват смарт карти, безконтактни карти и карти с чип. Ако една от тези карти и съответният четец за карти са свързани към компютъра, ако администраторът е инсталирал съответния драйвер от производителя и ако администраторът е разрешил картата като вид идентификационни данни за удостоверяване, можете да използвате картата като идентификационни данни за удостоверяване.

При смарт картите производителят трябва да предостави инструменти за инсталиране на сертификат за защита и управление на PIN, които HP Client Security използва в защитния си алгоритъм. Броят и видът на символите, използвани като PIN код, може да е различен. Администраторът трябва да инициализира смарт картата преди да се използва.

Поддържат се следните формати на смарт карти от HP Client Security:

- CSP
- PKCS11

Поддържат се следните видове безконтактни карти от HP Client Security:

- Безконтактни HID iCLASS карти с памет
- Безконтактни MiFare Classic 1k, 4k, и мини карти с памет

Поддържат се следните карти с чип от HP Client Security:

- HID карти с чип

За да регистрирате смарт карта:

1. Поставете картата в свързания четец за смарт карти.
2. Когато картата бъде разпозната, въведете PIN кода на картата и щракнете или натиснете **Enroll** (Регистрация).

За да смените PIN код на смарт карта:

1. Поставете картата в свързания четец за смарт карти.
2. Когато картата бъде разпозната, въведете PIN кода на картата и щракнете или натиснете **Authenticate** (Удостоверяване).
3. Щракнете или натиснете **Change PIN** (Промяна на PIN), а след това въведете новия PIN код.

За да регистрирате безконтактна карта или карта с чип:

1. Поставете картата много близо до съответния четец.
2. Когато картата е разпозната, щракнете или натиснете **Enroll** (Регистрация).

За изтриване на регистрирана карта:

1. Поставете карта в четеца.
2. Само при смарт карти, въведете PIN кода на картата и щракнете или натиснете **Authenticate** (Удостоверяване).
3. Щракнете или натиснете **Delete** (Изтриване).

След като картата е регистрирана, подробностите за картата са показани в **Регистрирани карти**. Когато картата е изтрита, тя се премахва от списъка.

За достъп до Настройки на карти с чип, безконтактни и смарт карти, където администраторът може да зададе настройки, свързани с идентификационните данни, щракнете или натиснете **Settings** (Настройки) (изисква административни права).

Настройки на карти с чип, безконтактни и смарт карти

За достъп до настройките на картата, щракнете или натиснете картата в списъка, после щракнете или натиснете показаната стрелка.

За да смените PIN код на смарт карта:

1. Поставете карта в четеца
2. Въведете PIN кода на картата и щракнете или натиснете **Continue** (Продължаване).
3. Въведете и потвърдете новия PIN код, после щракнете или натиснете **Continue** (Продължаване).

За инициализиране на PIN код на смарт карта:

1. Поставете карта в четеца
2. Въведете PIN кода на картата и щракнете или натиснете **Continue** (Продължаване).
3. Въведете и потвърдете новия PIN код, после щракнете или натиснете **Continue** (Продължаване).
4. Щракнете или натиснете **Yes** (Да), за да потвърдите инициализацията.

За да изчистите данни от карта:

1. Поставете карта в четеца
2. Въведете PIN кода на картата (само за смарт карти) и щракнете или натиснете **Continue** (Продължаване).
3. Щракнете или натиснете **Yes** (Да), за да потвърдите изтриването.

PIN

Ако администраторът е разрешил PIN код като начин за въвеждане на идентификационни данни за удостоверяване, можете да конфигурирате PIN код в комбинация с други идентификационни данни за допълнителна защита.

За конфигуриране на нов PIN:

▲ Въведете PIN кода, въведете го отново за потвърждение, после щракнете или натиснете **Apply** (Прилагане).

За изтриване на PIN:

▲ Щракнете или натиснете **Delete** (Изтриване), а след това щракнете или натиснете **Yes** (Да), за да потвърдите.

За достъп до настройките на PIN, където администраторът може да зададе настройки, свързани с идентификационните данни за PIN, щракнете или натиснете **Настройки** (изисква административни права).

Настройки на PIN

От страницата Настройки на PIN можете да зададете минималната и максимална допустима дължина за идентификация с PIN код.

RSA SecurID

Ако администраторът е разрешил RSA като вид идентификационни данни за удостоверяване и следните условия са изпълнени, можете да регистрирате или изтриете идентификация чрез RSA SecurID.

ЗАБЕЛЕЖКА: Изисква се съответната конфигурация.

- Потребителят трябва да е създаден на RSA сървър.
- На потребителя трябва да е назначен RSA SecurID маркер и компютърът трябва да е включен в домейн с RSA сървър.
- SecurID софтуерът е инсталиран на компютъра.
- Налична е връзка с правилно конфигуриран RSA сървър.

За регистриране на RSA SecurID идентификация:

▲ Въведете вашето потребителско име и код за достъп за RSA SecurID (RSA SecurID кода на маркера или PIN+кода на маркера, в зависимост от вашата среда), после щракнете или натиснете **Прилагане**.

При успешна регистрация се показва съобщение „Your RSA SecurID credential has been successfully enrolled“ (Вашата RSA SecurID идентификация е регистрирана успешно) и бутонът „Изтриване“ става активен.

За изтриване на RSA SecurID идентификация:

▲ Щракнете върху **Изтриване**, после изберете **Да** в прозореца, който ви пита “Наистина ли искате да изтриете вашата RSA SecurID идентификация?”

Password Manager

Влизането в уеб сайтове и приложения е по-лесно и по-сигурно, когато използвате Password Manager. Можете да създадете по-силни пароли, които не е нужно да записвате или помните,

после да влезете лесно и бързо с пръстов отпечатък, смарт карта, карта с чип, безконтактна карта, Bluetooth телефон, PIN код, RSA идентификация или с вашата парола за Windows.

ЗАБЕЛЕЖКА: Поради вечно променящата се структура на екраните за влизане в уеб, Password Manager може да не поддържа винаги всички уеб сайтове.

Password Manager предлага следните опции:

Password Manager страница

- Щракнете или натиснете акаунт, за да стартирате автоматично уеб страница или приложение и да влезете.
- Използвайте категории, за да организирате вашите акаунти.

Сила на парола

- Вижте веднага дали някоя от вашия пароли представлява риск за защитата.
- Когато добавяте данни за влизане, проверете силата на отделните пароли, използвани за уеб сайтове и приложения.
- Силата на паролата е показана с червени, жълти и зелени индикатори на състоянието.

Иконата на **Password Manager** е показана в горния ляв ъгъл в екрана за влизане в уеб страница или приложение. Когато още не е създадено влизане за тази уеб страница или приложение, на иконата има показан знак плюс.

▲ Щракнете или натиснете иконата на **Password Manager**, за да се покаже контекстно меню, където можете да изберете между следните опции:

- Добавяне на [somedomain.com] към Password Manager
- Отваряне на Password Manager
- Настройки на икона
- Помощ

За уеб страници или програми, за които още не е създадено влизане

В контекстното меню се показват следните опции:

- **Добавяне на [somedomain.com] към Password Manager**—Позволява ви да добавите влизане за текущия екран за влизане.
- **Отваряне на Password Manager**—Стартира Password Manager.
- **Настройки на икона**—Позволява да укажете условията, при които се показва иконата на **Password Manager**.
- **Помощ**—Показва Помощ за HP Client Security.

За уеб страници или програми, за които вече е създадено влизане

В контекстното меню се показват следните опции:

- **Попълване на данни за влизане**—Показва страницата **Потвърдете вашата самоличност**. Ако се се удостоверили успешно, вашите данни за влизане се поставят в полетата за влизане, после страницата се изпраща (ако е указано изпращане при създаването или последната редакция на влизането).
- **Редактиране на влизане**—Позволява да редактирате данните за влизане на този уеб сайт.
- **Добавяне на влизане**—Позволява добавяне на акаунт към Password Manager.
- **Отваряне на Password Manager**—Стартира Password Manager.
- **Помощ**—Показва Помощ за HP Client Security.

ЗАБЕЛЕЖКА: Администраторът на този компютър може да е конфигурирал HP Client Security да изисква повече от едни идентификационни данни при потвърждаване на вашата самоличност.

Добавяне на влизане

Можете лесно да добавите влизане за уеб сайт или програма, като въведете еднократно информацията за влизане. След това Password Manager автоматично ще въвежда информацията вместо вас. Можете да използвате тези данни за влизане след като сърфирате в уеб сайтове или програма.

За да добавите влизане:

1. Отворете екрана за влизане на уеб сайта или програмата.
2. Щракнете или натиснете иконата на **Password Manager**, после щракнете или натиснете едно от следните, в зависимост дали екранът за влизане е за уеб сайт или програма:
   - За уеб сайт щракнете или натиснете **Добавяне на [име на домейн] към Password Manager**.
   - За програма щракнете или натиснете **Добавяне на този екран за влизане към Password Manager**.
3. Въведете вашите данни за влизане. Полетата за влизане на екрана и съответните полета в диалоговия прозорец са указани с дебела оранжева линия.
   а. За да попълните полето за влизане с един от предварително форматираните избори, щракнете или натиснете стрелките отдясно на полето.
   б. За да видите паролата за това влизане, щракнете или натиснете **Показване на парола**.
   в. За да се попълнят полетата за влизане, но да не се изпратят, махнете отметката **Automatically submit logon data** (Автоматично изпращане на данни за влизане).
   г. Щракнете или натиснете **OK**, за да изберете начина за удостоверяване, който искате да използвате (пръстови отпечатъци, смарт карта, карта с чип, безконтактна карта,

Bluetooth телефон, PIN код или парола), после влезте по избрания начин за удостоверяване.

Знакът плюс изчезва от иконата на **Password Manager**, за да укаже, че влизането е създадено.

д. Ако Password Manager не намери полета за влизане, щракнете или натиснете **More fields** (Още полета).

- Изберете отметката за всяко поле, което се изисква при влизане, или махнете отметката за всяко поле, което не се изисква за влизане.
- Щракнете или натиснете **Close** (Затваряне).

Всеки път, когато посетите този уеб сайт или отворите тази програма, иконата на **Password Manager** се показва в горния ляв ъгъл на екрана за влизане на уеб сайта или програмата, което показва, че можете да използвате вашите регистрирани идентификационни данни за влизане.

Редактиране на данни за влизане

За да редактирате влизане:

1. Отворете екрана за влизане на уеб сайта или програмата.
2. За да се покаже диалогов прозорец, в който можете да редактирате информацията за влизане, щракнете или натиснете иконата на **Password Manager**, после щракнете или натиснете **Edit Logon** (Редактиране на влизане).

   Полетата за влизане на екрана и съответните полета в диалоговия прозорец са указани с дебела оранжева линия.

   Можете също да редактирате информацията за акаунта от страницата на Password Manager, като щракнете или натиснете върху данните за влизане, за да се покажат опциите за редактиране, а след това изберете **Edit** (Редактиране).
3. Редактиране на информация за влизане.
   - За да редактирате **Account name** (Име на акаунт), въведете ново име в полето.
   - За да добавите или редактирате име на **Category** (Категория), въведете или променете името в полето **Category** (Категория).
   - За да изберете в полето за влизане **Username** (Потребителско име) един от предварително форматираните избори, щракнете или натиснете стрелката отдясно на полето.

     Предварително форматираните избори са налични само когато редактирате влизането от командата Edit (Редактиране) в контекстното меню на иконата Password Manager.
   - За да изберете в полето за влизане **(Password)** (Парола) един от предварително форматираните избори, щракнете или натиснете стрелката отдясно на полето.

     Предварително форматираните избори са налични само когато редактирате влизането от командата Edit (Редактиране) в контекстното меню на иконата Password Manager.
   - За да добавите допълнителни полета от екрана във вашето влизане, щракнете или натиснете **More fields** (Още полета).

- За да видите паролата за това влизане, щракнете или натиснете иконата **Show password** (Показване на парола).
- За да се попълнят полетата за влизане, но да не се изпратят, махнете отметката **Automatically submit logon data** (Автоматично изпращане на данни за влизане).
- За да маркирате паролата за това влизане като компрометирана, изберете отметката **Тази парола е компрометирана**.

  След като запишете промените, всички други данни за влизане, които споделят същата парола, също ще бъдат маркирани като компрометирани. Тогава можете да посетите всеки засегнат акаунт и да смените паролите, ако е необходимо.

4. Щракнете или натиснете **OK**.

Използване на менюто Бързи връзки в Password Manager

Password Manager предоставя бърз и лесен начин за стартиране на уебсайтове и програми, за които сте създали влизане. Щракнете двукратно или натиснете двукратно влизането за програма или уеб сайт от менюто **Бързи връзки в Password Manager** или от страницата Password Manager в HP Client Security, за да отворите екран за влизане, после попълнете вашите данни за влизане.

Когато създадете влизане, то автоматично се добавя в менюто **Бързи връзки** в Password Manager.

За да се покаже менюто **Бързи връзки**:

▲ Натиснете клавишната комбинация за **Password Manager** (Ctrl+клавиш Windows+h е фабричната настройка). За да промените клавишната комбинация, от началната страница на HP Client Security щракнете върху **Password Manager**, после щракнете или натиснете **Настройки**.

Организиране на данните за влизане в категории

Създайте една или повече категории, за да подредите данните за влизане.

За да отнесете данните за влизане към категория:

1. От началната страница на HP Client Security щракнете или натиснете **Password Manager**.
2. Щракнете или натиснете запис за акаунт, после щракнете или натиснете **Edit** (Редактиране).
3. В полето **Category** (Категория) въведете име на категорията.
4. Щракнете или натиснете **Save** (Запис).

За да премахнете акаунт от категория:

1. От началната страница на HP Client Security щракнете или натиснете **Password Manager**.
2. Щракнете или натиснете запис за акаунт, после щракнете или натиснете **Edit** (Редактиране).
3. В полето **Category** (Категория) изтрийте името на категорията.
4. Щракнете или натиснете **Save** (Запис).

За да преименувате категория:

1. От началната страница на HP Client Security щракнете или натиснете **Password Manager**.
2. Щракнете или натиснете запис за акаунт, после щракнете или натиснете **Edit** (Редактиране).
3. В полето **Category** (Категория) сменете името на категорията.
4. Щракнете или натиснете **Save** (Запис).

Управление на данните за влизане

С Password Manager лесно и централизирано управлявате вашата информация за влизане като потребителски имена, пароли и множество акаунти за влизане.

Вашите влизания са изброени на страницата Password Manager.

За да управлявате вашите влизания:

1. От началната страница на HP Client Security щракнете или натиснете **Password Manager**.
2. Щракнете или натиснете съществуващо влизане, после изберете една от следните опции и следвайте указанията на екрана:
   - **Edit** (Редактиране)—Редактиране на данни за влизане. За повече информация вж. Редактиране на данни за влизане на страница 22.
   - **Log in** (Влизане)—Влизане в избран акаунт.
   - **Delete** (Изтриване)—Изтриване на данни за влизане за избран акаунт.

За да добавите допълнително влизане към уеб сайт или програма:

1. Отворете екрана за влизане на уеб сайта или програмата.
2. Щракнете или натиснете иконата на **Password Manager**, за да се покаже контекстното меню.
3. Щракнете или натиснете **Добавяне на влизане** и следвайте указанията на екрана.

Оценка на силата на вашата парола

Използването на силни пароли за влизане в уеб сайтове и програми е важна част от защитата на вашата самоличност.

С Password Manager лесно наблюдавате и подобрявате вашата защита с незабавен и автоматичен анализ на силата на всяка от паролите, използвани за влизане в уеб сайтове и програми.

Докато въвеждате парола при създаването на влизане през Password Manager за даден акаунт, под паролата се показва цветна лента, която указва силата на паролата. Цветовете показват следните стойности:

- **Червен**—Слаба
- **Жълт**—Задоволителна
- **Зелен**—Силна

Настройки на икона на Password Manager

Password Manager се опитва да идентифицира екраните за влизане в уеб сайтове и програми. Когато открие екран за влизане, за който не сте създали данни за влизане, Password Manager

ви подканя да добавите данни за влизане за този екран, като показва иконата на **Password Manager** със знак плюс.

1. Щракнете или натиснете иконата, после щракнете или натиснете **Настройки на икона**, за да персонализирате начина, по който Password Manager обработва възможните сайтове за влизане.

   - **Искане за добавяне на влизане в екрани за влизане**—Щракнете или натиснете тази опция, за да ви пита Password Manager дали да добави влизане при показване на екран за влизане, за който още не е настроено влизане.
   - **Изключване на този екран**—Изберете отметката, за да не ви пита Password Manager отново дали да добави влизане за този екран за влизане.
   - **Не питай за добавяне на влизане в екрани за влизане**—Изберете радио бутона.

2. За да добавите влизане за екран, който е бил изключен преди това:

   а. Влезте в изключения преди това уеб сайт.

   б. За да може Password Manager да запомни паролата за този сайт, щракнете или натиснете **Remember** (Запомни ме) на изскачащия диалогов прозорец, за да запазите паролата и да създадете данни за влизане за екрана.

3. За достъп до допълнителни настройки на Password Manager щракнете или натиснете иконата на Password Manager, щракнете или натиснете **Open Password Manager** (Отваряне на Password Manager), а след това щракнете или натиснете **Settings** (Настройки) на страницата на Password Manager.

Импортиране и експортиране на данни за влизане

От страницата HP Password Manager импорт и експорт можете да импортирате данните за влизане, записани от уеб браузърите на вашия компютър. Можете също да импортирате данни от архивен файл на HP Client Security и да експортирате данни в архивен файл на HP Client Security.

▲ За да стартирате страницата за импорт и експорт, щракнете или натиснете **Import and export** (Импорт и експорт) на страницата на Password Manager.

За да импортирате пароли от браузър:

1. Щракнете или натиснете браузъра, от който искате да импортирате пароли (показват се само инсталираните браузъри).
2. Махнете отметката от всички акаунти, за които не искате да импортирате пароли.
3. Щракнете или натиснете **Импортиране**.

Импортиране или експортиране на данни в архивен файл на HP Client Security може да се извърши чрез съответните връзки (от **Други опции)** на страницата Импорт и експорт.

ЗАБЕЛЕЖКА: Тази функция импортира и експортира само данни за Password Manager. За информация относно архивиране и възстановяване на допълнителни данни за HP Client Security, вижте Архивиране и възстановяване на вашите данни на страница 30.

За да импортирате данни от архивен файл на HP Client Security:

1. От страницата HP Password Manager за импорт и експорт щракнете или натиснете **Import data from an HP Client Security backup file** (Импортиране на данни от архивен файл на HP Client Security).
2. Потвърдете своята самоличност.

3. Изберете създаден преди това архивен файл или въведете пътя в предоставеното поле, после щракнете или натиснете **Browse** (Преглед).
4. Въведете паролата за защита на файла, после щракнете или натиснете **Next** (Напред).
5. Щракнете или натиснете **Restore** (Възстановяване).

За да експортирате данни в архивен файл на HP Client Security:

1. От страницата HP Password Manager Импорт и експорт щракнете или натиснете **Експорт на данни от архивен файл на HP Client Security**.
2. Потвърдете своята самоличност, после щракнете или натиснете **Напред**.
3. Въведете име за архивния файл. По подразбиране файлът се записва в папката Документи. За да укажете друго местоположение, щракнете или натиснете **Browse** (Преглед).
4. Въведете и потвърдете парола за защита на файла, после щракнете или натиснете **Save** (Запис).

Настройки

Можете да зададете настройки за персонализиране на Password Manager:

- **Искане за добавяне на влизане в екрани за влизане**—Когато бъде открит екран за влизане за уеб сайт или програма, се показва иконата на **Password Manager** със знак плюс, което означава, че можете да добавите влизане за този екран в менюто **Влизания**.

  За да забраните тази функция, махнете отметката до **Искане за добавяне на влизане в екрани за влизане**.

- **Отворете Password Manager с Ctrl+Win+h**—Клавишната комбинация по подразбиране, която отваря **менюто за бързи връзки на Password Manager** е Ctrl+клавиш Windows+h.

  За да смените клавишната комбинация, щракнете или натиснете тази опция, после въведете нова клавишна комбинация. Комбинациите могат да включват един или повече от следните: ctrl, alt, или shift, както и всеки клавиш с буква или цифра.

  Комбинациите, запазени за Windows или Windows приложения, не могат да се използват.

- За да върнете настройките до фабричните настройки по подразбиране, щракнете или натиснете **Restore defaults** (Възстановяване на настройките по подразбиране).

Разширени настройки

Администраторите имат достъп до следните опции, когато изберат иконата **Gear** (настройки) в началната страница на HP Client Security.

- **Правила за администратори**—Позволява конфигурирането на правила за влизане и сесии за администратори.
- **Правила за стандартни потребители**—Позволява конфигурирането на правила за влизане и сесии за стандартни потребители.
- **Функции за защита**—Позволява повишаване на защитата на компютъра, като защитава вашия акаунт за Windows чрез засилено удостоверяване и/или чрез разрешаване на удостоверяване преди стартиране на Windows.
- **Потребители**—Позволява ви да управлявате потребителите и техните идентификационни данни.

- **Мои правила**—Позволява преглед на правилата за удостоверяване и състоянието на регистрациите.
- **Архивиране и възстановяване**—Позволява да архивирате или възстановите HP Client Security данни.
- **Относно HP Client Security**—Показва информация за версията на HP Client Security.

Правила за администратори

Можете да конфигурирате правила за влизане и сесии за администраторите на този компютър. Настроените тук правила за влизане управляват идентификационните данни, които се изискват за влизане на локалния администратор в Windows. Настроените тук правила за сесии управляват идентификационните данни, които се изискват за проверка на самоличността на локалния администратор в Windows сесия.

По подразбиране всички нови или променени правила влизат в сила незабавно след щракване или натискане на **Прилагане**.

За да добавите ново правило:

1. От началната страница на HP Client Security щракнете или натиснете иконата **Gear** (настройки).
2. От страницата Разширени настройки щракнете или натиснете **Administrator Policies** (Правила за администратори).
3. Щракнете или натиснете **Add new policy** (Добавяне на ново правило).
4. Щракнете върху стрелките надолу, за да изберете първични и (опционално) вторични идентификационни данни за новото правило, после щракнете или натиснете **Add** (Добавяне).
5. Щракнете върху **Apply** (Приложи).

За да отложите влизането в сила на новото или променено правило:

1. Щракнете или натиснете **Enforce this policy immediately** (Прилагане на това правило незабавно).
2. Изберете **Enforce this policy on the specific date** (Прилагане на това правило на конкретна дата).
3. Въведете дата или използвайте календара, за да изберете дата на влизане в сила на правилото.
4. Ако искате, изберете кога да напомните на потребителите за ново правило.
5. Щракнете върху **Apply** (Приложи).

Правила за стандартни потребители

Можете да конфигурирате правила за влизане и сесии за стандартните потребители на този компютър. Настроените тук правила за влизане управляват идентификационните данни, които се изискват за влизане на стандартен потребител в Windows. Настроените тук правила за сесии управляват идентификационните данни, които се изискват за проверка на самоличността на стандартен потребител в Windows сесия.

По подразбиране всички нови или променени правила влизат в сила незабавно след щракване или натискане на **Прилагане**.

За да добавите ново правило:

1. От началната страница на HP Client Security щракнете или натиснете иконата **Gear** (настройки).
2. От страницата Разширени настройки щракнете или натиснете **Standard User Policies** (Правила за стандартни потребители).
3. Щракнете или натиснете **Add new policy** (Добавяне на ново правило).
4. Щракнете върху стрелките надолу, за да изберете първични и (опционално) вторични идентификационни данни за новото правило, после щракнете или натиснете **Add** (Добавяне).
5. Щракнете върху **Apply** (Приложи).

За да отложите влизането в сила на новото или променено правило:

1. Щракнете или натиснете **Enforce this policy immediately** (Прилагане на това правило незабавно).
2. Изберете **Enforce this policy on the specific date** (Прилагане на това правило на конкретна дата).
3. Въведете дата или използвайте календара, за да изберете дата на влизане в сила на правилото.
4. Ако искате, изберете кога да напомните на потребителите за ново правило.
5. Щракнете върху **Apply** (Приложи).

Функции за защита

Можете да разрешите Функциите за защита на HP Client Security, които помагат за предотвратяване на неразрешен достъп до компютъра.

За да конфигурирате функции за защита:

1. От началната страница на HP Client Security щракнете или натиснете иконата **Gear** (настройки).
2. От страницата Разширени настройки щракнете или натиснете **Security Features** (Функции за защита).

3. Разрешете функциите за защита, като изберете отметките и после щракнете или натиснете **Apply** (Прилагане). Колкото повече функции изберете, толкова по-защитен ще бъде вашият компютър.

   Тези настройки важат за всички потребители.

   - **Защита при влизане в Windows**—Защитава вашият акаунт в Windows, като изисква използването на данни за идентификация от HP Client Security за достъп.
   - **Защита преди зареждане (Удостоверяване при включване)**—Защитава вашия компютър преди стартиране на Windows. Този избор не е наличен, ако BIOS не го поддържа.
   - **Разрешаване на влизане с едно действие**—Тази настройка позволява прескачане на влизането в Windows, ако преди това е било извършено удостоверяване при включване или в Drive Encryption.

4. Щракнете или натиснете **Users** (Потребители), а след това щракнете или натиснете плочката на потребителя.

Потребители

Можете да наблюдавате и управлявате потребителите на HP Client Security на този компютър.

За да добавите друг Windows потребител към HP Client Security:

1. От началната страница на HP Client Security щракнете или натиснете иконата **Gear** (настройки).
2. От страницата Разширени настройки щракнете или натиснете **Users** (Потребители).
3. Щракнете или натиснете **Add another Windows user to HP Client Security** (Добавяне на друг Windows потребител към HP Client Security).
4. Въведете името на потребителя, който искате да добавите, после щракнете или натиснете **OK**.
5. Въведете паролата за Windows на потребителя.

   На страницата Потребители се показва плочка за добавения потребител.

За да изтриете Windows потребител от HP Client Security:

1. От началната страница на HP Client Security щракнете или натиснете иконата **Gear** (настройки).
2. От страницата Разширени настройки щракнете или натиснете **Users** (Потребители).
3. Щракнете или натиснете името на потребителя, който искате да изтриете.
4. Щракнете или натиснете **Delete User** (Изтриване на потребител), а след това щракнете или натиснете **Yes** (Да), за да потвърдите.

За да се покаже обобщение на правилата за влизане и сесии, приложени към потребителя:

▲ Щракнете или натиснете **Users** (Потребители), а след това щракнете или натиснете плочката на потребителя.

Мои правила

Можете да покажете вашите правила за удостоверяване и статус на регистрация. Страницата Мои правила предоставя и връзки към страниците Правила за администратори и Правила за стандартни потребители.

1. От началната страница на HP Client Security щракнете или натиснете иконата **Gear** (настройки).
2. От страницата Разширени настройки щракнете или натиснете **My Policies** (Мои правила).

   Показват се правилата за влизане и сесии, които са в сила за текущо влезлия потребител.

Страницата Мои правила предоставя и връзки към Правила за администратори на страница 27 и Правила за стандартни потребители на страница 27.

Архивиране и възстановяване на вашите данни

Препоръчително е да архивирате редовно вашите HP Client Security данни. Честотата на архивиране зависи от честотата на промените на данните. Например, ако добавяте нови влизания всеки ден, трябва да архивирате вашите данни всеки ден.

Архивите могат да се използват и за мигриране от един компютър на друг, също наричано импортиране и експортиране.

ЗАБЕЛЕЖКА: Тази функция архивира само Password Manager. Drive Encryption има отделен начин за архивиране. Device Access Manager и информацията за удостоверяване с пръстов отпечатък не се архивират.

HP Client Security трябва да е инсталиран на компютъра, който трябва да приеме архивираните данни, преди те да могат да бъдат възстановени от архивния файл.

За да архивирате вашите данни:

1. От началната страница на HP Client Security щракнете или натиснете иконата **Gear** (настройки).
2. От страницата Разширени настройки щракнете или натиснете **Administrator Policies** (Правила за администратори).
3. Щракнете или натиснете **Backup and Restore** (Архивиране и възстановяване).
4. Щракнете или натиснете **Backup** (Архивиране), а след това потвърдете вашата самоличност.
5. Изберете модула, който искате да включите в архива, после щракнете или натиснете **Next** (Напред).
6. Въведете име за файла за съхраняване на данни. По подразбиране файлът се записва в папката Документи. За да укажете друго местоположение, щракнете или натиснете **Browse** (Преглед).
7. Въведете и потвърдете парола за защита на файла.
8. Щракнете или натиснете **Save** (Запис).

За да възстановите вашите данни:

1. От началната страница на HP Client Security щракнете или натиснете иконата **Gear** (настройки).
2. От страницата Разширени настройки щракнете или натиснете **Administrator Policies** (Правила за администратори).
3. Щракнете или натиснете **Backup and Restore** (Архивиране и възстановяване).
4. Изберете **Restore** (Възстановяване), а след това потвърдете вашата самоличност.
5. Изберете създаден преди това файл за съхраняване на данни. Въведете пътя в предоставеното поле. За да укажете друго местоположение, щракнете или натиснете **Browse** (Преглед).
6. Въведете паролата за защита на файла, после щракнете или натиснете **Next** (Напред).
7. Изберете модулите, за които искате са възстановите данни.
8. Щракнете или натиснете **Restore** (Възстановяване).

5 HP Drive Encryption (само при определени модели)

HP Drive Encryption предоставя пълна защита на данните чрез шифроване на данните на вашия компютър. При активиране на Drive Encryption, вие трябва да влезете на екрана за влизане на Drive Encryption, който се показва преди стартиране на операционната система Windows® .

Началният екран на HP Client Security позволява на администраторите на Windows да активират Drive Encryption, да създадат резервен ключ за шифроване и да изберат или да отменят избора на диск(ове) или дял(ове) за шифроване. За повече информация вижте Помощ в софтуера HP Client Security.

С Drive Encryption могат да се изпълняват следните задачи:

- Избор на настройки за Drive Encryption:
  - Шифроване или дешифриране на отделни дискове или дялове чрез софтуерно шифроване
  - Шифроване или дешифриране на отделни дискове със самостоятелно шифроване чрез хардуерно шифроване
  - Добавянето на допълнителна защита чрез забрана на Заспиване или Режим на готовност, за да се гарантира, че винаги се изисква удостоверяване преди зареждане през Drive Encryption

ЗАБЕЛЕЖКА: Могат да бъдат шифровани само вътрешни SATA и външни eSATA твърди дискове.

- Създаване на резервни ключове
- Възстановяване на достъп до шифрован компютър с използване на резервни ключове и HP SpareKey
- Активиране на удостоверяване преди зареждане през Drive Encryption с помощта на парола, регистриран пръстов отпечатък или PIN за избрани смарт карти

Отваряне на Drive Encryption

Администраторите имат достъп до Drive Encryption, като отворят HP Client Security:

1. От стартовия екран щракнете или натиснете приложението **HP Client Security** (Windows 8).

   – или –

   От работния плот на Windows щракнете двукратно или натиснете двукратно иконата **HP Client Security** в областта за уведомяване, разположена най-вдясно на лентата със задачи.

2. Щракнете или натиснете иконата **Drive Encryption**.

Общи задачи

Активиране на Drive Encryption за стандартни твърди дискове

Стандартните твърди дискове са шифровани със софтуерно шифроване. Следвайте тези стъпки, за да шифровате диск или дял от диск:

1. Стартирайте **Drive Encryption**. За повече информация вж. Отваряне на Drive Encryption на страница 32.
2. Изберете отметката за диска или дяла, който искате да шифровате, после щракнете или натиснете **Резервен ключ**.

ЗАБЕЛЕЖКА: За повишена защита изберете отметката **Забрана на режим заспиване за повишена защита**. Когато забраните режима на заспиване, няма опасност вашите идентификационни данни за отключване на диска да бъдат записани в паметта.

3. Изберете една или повече опции за архивиране, после щракнете или натиснете **Архивиране**. За повече информация вж. Архивиране на ключове за шифроване на страница 36.
4. Можете да продължите да работите, докато ключът за шифроване се архивира. Не рестартирайте компютъра.

ЗАБЕЛЕЖКА: Появява се искане да рестартирате компютъра. След рестарта се показва екранът за стартиране преди зареждане през Drive Encryption, който изисква удостоверяване преди стартиране на Windows.

Drive Encryption е активиран. Шифроването на избраните дял(ове) от диска може да отнеме няколко часа, в зависимост от броя и размера на дял(овете).

За повече информация вижте Помощ в софтуера HP Client Security.

Активиране на Drive Encryption за дискове със самостоятелно шифроване

Дисковете за самостоятелно шифроване, които отговарят на спецификацията на Trusted Computing Group OPAL за управление на дискове със самостоятелно шифроване, могат да бъдат шифровани със софтуерно или хардуерно шифроване. Хардуерното шифроване е много по-бързо от софтуерното. Но не можете да избирате кои дялове от диска да шифровате. Шифрова се целият диск, включително всички дялове.

За да шифровате конкретни дялове, трябва да използвате софтуерно шифроване. Уверете се, че сте премахнали отметката **Позволяване само на хардуерно шифроване за дискове със самостоятелно шифроване (SEDs)**.

Следвайте тези стъпки, за да активирате Drive Encryption за дискове със самостоятелно шифроване:

1. Стартирайте **Drive Encryption**. За повече информация вж. Отваряне на Drive Encryption на страница 32.
2. Изберете отметката за диска, който искате да шифровате, после щракнете или натиснете **Резервен ключ**.

ЗАБЕЛЕЖКА: За повишена защита изберете отметката **Забрана на режим заспиване за повишена защита**. Когато забраните режима на заспиване, няма опасност вашите идентификационни данни за отключване на диска да бъдат записани в паметта.

3. Изберете една или повече опции за архивиране, после щракнете или натиснете **Архивиране**. За повече информация вж. Архивиране на ключове за шифроване на страница 36.

4. Можете да продължите да работите, докато ключът за шифроване се архивира. Не рестартирайте компютъра.

ЗАБЕЛЕЖКА: При дискове със самостоятелно шифроване ще получите искане да изключите компютъра.

За повече информация вижте Помощ в софтуера HP Client Security.

Деактивиране на Drive Encryption

1. Стартирайте **Drive Encryption**. За повече информация вж. Отваряне на Drive Encryption на страница 32.

2. Премахнете отметката от всички шифровани дискове и щракнете или натиснете **Прилагане**.

   Деактивирането на Drive Encryption започва.

ЗАБЕЛЕЖКА: Ако е било използвано софтуерно шифроване, дешифрирането започва. Може да отнеме няколко часа, в зависимост от размера на шифрованите дял(ове) на твърдия диск. Когато дешифрирането приключи, Drive Encryption е деактивиран.

Ако е било използвано хардуерно шифроване, дискът се дешифрира незабавно и след няколко минути Drive Encryption е деактивиран.

След деактивиране на Drive Encryption ще получите искане за изключване на компютъра ако е бил хардуерно шифрован, или да го рестартирате, ако е бил софтуерно шифрован.

Влизане след активиране на Drive Encryption

Когато включите компютъра след активиране на Drive Encryption и вашият потребителски акаунт е регистриран, трябва да влезете през екрана за влизане на Drive Encryption:

ЗАБЕЛЕЖКА: Когато компютърът се събужда след заспиване или режим на готовност, удостоверяването преди зареждане през Drive Encryption не се показва за софтуерно или хардуерно шифроване. Хардуерното шифроване предоставя опцията **Забрана на режим заспиване за повишена защита**, при активирането на която не се позволява влизане в режимите заспиване или готовност.

Когато компютърът се събужда след хибернация, удостоверяването преди зареждане през Drive Encryption се показва и за софтуерно и за хардуерно шифроване.

ЗАБЕЛЕЖКА: Ако администраторът на Windows е разрешил BIOS защита преди зареждане в HP Client Security и Влизане с едно действие е разрешено (по подразбиране), можете да влезете в компютъра незабавно след като се удостоверите в BIOS защитата преди зареждане, без да е необходимо да се удостоверявате отново в екрана за влизане на Drive Encryption.

Влизане на един потребител:

- На страницата за **Влизане** въведете вашата парола за Windows, PIN на смарт карта, SpareKey или плъзнете регистриран пръст.

Влизане на няколко потребители:

1. На страницата **Избор на влизане за потребител** изберете потребителя, който ще влиза, от падащия списък, после щракнете или натиснете **Напред**.
2. На страницата за **Влизане** въведете вашата парола за Windows, PIN на смарт карта или плъзнете регистриран пръст.

ЗАБЕЛЕЖКА: Поддържат се следните смарт карти:

Поддържани смарт карти

- Gemalto Cyberflex Access 64k V2c

ЗАБЕЛЕЖКА: Ако се използва ключът за възстановяване в екрана за влизане на Drive Encryption, се изискват допълнителни идентификационни данни при влизането в Windows за достъп до потребителските акаунти.

Шифроване на допълнителни твърди дискове

Силно препоръчително е да използвате HP Drive Encryption за защита на вашите данни чрез шифроване на вашия твърд диск. След активация всички добавени твърди дискове или създадени дялове могат да се шифроват, като се следват тези стъпки:

1. Стартирайте **Drive Encryption**. За повече информация вж. Отваряне на Drive Encryption на страница 32.
2. За софтуерно шифровани дискове, изберете дяловете на дисковете, които ще шифровате.

ЗАБЕЛЕЖКА: Това важи също и за случай на смесени дискове, когато има един или повече стандартни твърди дискове и един или повече дискове със самостоятелно шифроване.

– или –

- За хардуерно шифровани дискове, изберете допълнителните диск(ове), които ще шифровате.

Разширени задачи

Управление на Drive Encryption (административна задача)

Администраторите могат да използват Drive Encryption за преглед и промяна на статуса на шифроване (шифрован или не е шифрован) на всички твърди дискове на компютъра.

- Ако има статус Разрешен, Drive Encryption е активиран и конфигуриран. Дискът е в едно от следните състояния:

Софтуерно шифроване

  - Не е шифрован
  - Шифрован
  - Шифроване
  - Дешифриране

Хардуерно шифроване

- Шифрован
- Не е шифрован (за допълнителни дискове)

Шифроването и дешифрирането на отделни дялове на дискове (само софтуерно шифроване)

Администраторите могат да използват Drive Encryption, за да шифроват един или повече дял(а) на твърд диск на компютъра или да дешифрират всеки дял, който вече е бил шифрован.

1. Стартирайте **Drive Encryption**. За повече информация вж. Отваряне на Drive Encryption на страница 32.
2. От **Статус на дял** изберете или махнете отметката до всеки от дяловете на твърд диск, които желаете да шифровате или дешифрирате и после щракнете или натиснете **Прилагане**.

ЗАБЕЛЕЖКА: Когато се шифрова или дешифрира дял, се показва лента за прогреса в проценти.

ЗАБЕЛЕЖКА: Не се поддържат динамични дялове. Ако даден дял е показан като наличен, но не може да бъде шифрован, когато бъде избран, той е динамичен. Динамичните дялове се получават при намаляване на дял с цел създаване на нов дял в Управление на дискове.

Показва се предупреждение, ако дялът ще бъде конвертиран в динамичен.

Управление на дискове

- **Псевдоним**—Можете да изберете имена на вашите дялове или дискове за по-лесна идентификация.
- **Прекъснати дискове**—Drive Encryption може да наблюдава дисковете, които са извадени от компютъра. Диск, който е изваден от компютъра, автоматично се премества в списъка Прекъснати. Ако дискът бъде върнат в системата, той отново се появява в списъка Свързани.
- Ако вече не се нуждаете от наблюдение или управление на прекъснат диск, можете да го изтриете от списъка Прекъснати.
- Drive Encryption остава активен, докато не бъдат премахнати всички отметки от свързаните дискове и списъкът Прекъснати не е празен.

Архивиране и възстановяване (административна задача)

Когато Drive Encryption е активиран, администраторите могат да използват страницата Архивиране на ключ за шифроване, за да архивират ключовете за шифроване на сменяеми носители и да извършат възстановяване.

Архивиране на ключове за шифроване

Администраторите могат да архивират ключа за шифроване за шифрован дял на сменяемо устройство за съхраняване на данни.

ВНИМАНИЕ: Пазете устройството за съхраняване на данни, което съдържа резервния ключ на сигурно място, защото ако забравите паролата, загубите вашата смарт карта или нямате регистриран пръст, това устройство е единственият ви достъп до компютъра. Мястото на съхранение също трябва да е защитено, защото устройството за съхраняване на данни предоставя достъп до Windows.

1. Стартирайте **Drive Encryption**. За повече информация вж. Отваряне на Drive Encryption на страница 32.
2. Изберете отметката за диска, после щракнете или натиснете **Резервен ключ**.
3. От **Създаване на резервен ключ за HP Drive Encryption** изберете една или повече от следните опции:
   - **Преносимо устройство за съхранение**—Изберете отметката, после изберете устройството за съхраняване на данни, където ще запишете ключа за шифроване.
   - **SkyDrive**—Изберете отметката. Трябва да сте свързани към Интернет. Влезте в Microsoft SkyDrive и щракнете или натиснете **Да**.

     ЗАБЕЛЕЖКА: За да използвате резервния ключ за HP Drive Encryption, който се съхранява в SkyDrive, трябва да го изтеглите от SkyDrive на сменяемо устройство за съхраняване на данни, после да поставите устройството в компютъра.
   - **TPM** (само за избрани модели)—Позволява ви да възстановите вашите данни с вашата TPM парола.

     ВНИМАНИЕ: Ако TPM е изчистен или компютърът е повреден, ще загубите достъп до архива. Ако бъде избран този метод, трябва да бъде избран още един метод за архивиране.
4. Щракнете или натиснете **Архивиране**.

   Ключът за шифроване се записва на устройството за съхраняване на данни, което сте избрали.

Възстановяване на достъп до активиран компютър с помощта на резервни ключове

Администраторите могат да възстановят с помощта на резервен Drive Encryption ключ, архивиран на сменяемо устройство за съхраняване на данни по време на активация или чрез избор на опцията **Резервен ключ** в Drive Encryption.

1. Поставете сменяемото устройство за съхраняване на данни, което съдържа вашия резервен ключ.
2. Включете компютъра.
3. Когато се появи диалоговият прозорец за влизане в HP Drive Encryption, щракнете или натиснете **Възстановяване**.
4. Въведете пътя или името, където се съдържа вашия резервен ключ и щракнете или натиснете **Възстановяване**.
5. Когато се появи диалоговият прозорец за потвърждение, щракнете или натиснете **OK**.

   Показва се екранът за влизане в Windows.

ЗАБЕЛЕЖКА: Ако се използва ключът за възстановяване в екрана за влизане на Drive Encryption, се изискват допълнителни идентификационни данни при влизането в Windows за достъп до потребителските акаунти. Силно препоръчително е да смените паролата след възстановяване.

Извършване на възстановяване с HP SpareKey

Възстановяването със SpareKey в Drive Encryption преди зареждане изисква да отговорите правилно на въпроси за защита, преди да получите достъп до компютъра. За повече информация относно настройка на възстановяване със SpareKey, вижте Помощ в софтуера HP Client Security.

За да изпълните възстановяване със HP SpareKey, ако забравите вашата парола:

1. Включете компютъра.
2. Когато се покаже страницата на HP Drive Encryption, отидете в страницата за влизане на потребители.
3. Щракнете върху **SpareKey**.

   ЗАБЕЛЕЖКА: Ако вашият SpareKey не е инициализиран в HP Client Security, бутонът **SpareKey** не е наличен.

4. Отговорете правилно на показаните въпроси, а след това щракнете върху **Влизане**.

   Показва се екранът за влизане в Windows.

ЗАБЕЛЕЖКА: Ако се използва SpareKey в екрана за влизане на Drive Encryption, се изискват допълнителни идентификационни данни при влизането в Windows за достъп до потребителските акаунти. Силно препоръчително е да смените паролата след възстановяване.

6 HP File Sanitizer (само при определени модели)

File Sanitizer ви позволява безопасно да унищожавате активи (например: лична информация или файлове, исторически или уеб данни или други информационни компоненти) на вътрешния твърд диск на компютъра и периодично да избелвате вътрешния твърд диск на компютъра.

File Sanitizer не може да се използва за почистване или избелване на следните видове устройства:

- Немагнитни твърди дискове (SSD), включително RAID томове, който са разпространени на SSD устройство
- Външни дискове, свързани чрез USB, Firewire или eSATA интерфейс

Ако се направи опит за унищожаване или избелване на SSD, се показва предупредително съобщение и операцията не се изпълнява.

Унищожаване

Унищожаването е различно от стандартното изтриване в Windows®. Когато унищожите актив с File Sanitizer, файловете се презаписват с безсмислени данни, което прави буквално невъзможно възстановяването на оригиналния актив. Простото действие за изтриване в Windows може да остави файла (или актива) непокътнат на твърдия диск или в състояние, в което могат да се използват съдебни методи за възстановяването му.

Можете да планирате време за унищожаване в бъдеще или ръчно да активирате унищожаването, като изберете иконата **File Sanitizer** от началния екран на HP Client Security, или като използвате иконата **File Sanitizer** на работния плот на Windows. За повече информация, вижте Настройка на график за унищожаване на страница 41, Унищожаване с десен бутон на страница 43 или Ръчно стартиране на унищожаване на страница 43.

ЗАБЕЛЕЖКА: Файл във формат .dll ще бъде унищожен или изтрит от системата само, ако е преместен в Кошчето.

Избелване на свободното пространство

Изтриването на актив в Windows не премахва напълно съдържанието на актива от вашия твърд диск. Windows изтрива само препратката към актива или мястото му на твърдия диск. Съдържанието на актива все още остава на твърдия диск, докато друг актив не презапише същата област на твърдия диск с нова информация.

Избелването на свободното пространство ви позволява сигурно да запишете случайни данни върху изтритите активи, което ще попречи на потребителите да видят оригиналното съдържание на изтрития актив.

ЗАБЕЛЕЖКА: Избелването на свободното пространство не предоставя допълнителна защита на унищожените активи.

Можете да зададете време за избелване на свободното пространство в бъдеще или ръчно да активирате избелването на свободното пространство или на унищожени преди това активи,

като изберете иконата **File Sanitizer** от началния екран на HP Client Security, или като използвате иконата **File Sanitizer** на работния плот на Windows. За повече информация, вижте Настройка на график за избелване на свободното пространство на страница 42, Ръчно стартиране на избелване на свободното пространство на страница 44 или Използване на иконата File Sanitizer на страница 43.

Отваряне на File Sanitizer

1. От стартовия екран щракнете или натиснете приложението **HP Client Security** (Windows 8).

   – или –

   От работния плот на Windows щракнете двукратно или натиснете двукратно иконата **HP Client Security** в областта за уведомяване, разположена най-вдясно на лентата със задачи.

2. От **Данни** щракнете или натиснете **File Sanitizer**.

– или –

▲ Щракнете двукратно или натиснете двукратно иконата **File Sanitizer** на работния плот на Windows.

– или –

▲ Щракнете с десен бутон или натиснете и задръжте иконата **File Sanitizer** на работния плот на Windows и изберете **Отваряне на File Sanitizer**.

Процедури за конфигуриране

Унищожаване—File Sanitizer сигурно изтрива или унищожава избраните категории активи.

1. От **Унищожаване** изберете отметката за всеки вид файл, който трябва да бъде унищожен, или махнете отметката, ако не желаете да унищожавате тези файлове.

   - **Кошче**—Унищожава всички обекти в кошчето.
   - **Временни системни файлове**—Унищожава всички файлове, намерени във временната системна папка. Търсят се следните променливи на средата в следния ред, и първият намерен път се приема за системна папка:
     - TMP
     - TEMP
   - **Временни интернет файлове**—Унищожава копия на уеб страници, изображения и мултимедия, записани от уеб браузърите за по-бързо преглеждане.
   - **Бисквитки**—Унищожава всички файлове, записани на компютъра от уеб сайтовете с цел запазване на предпочитанията, например информация за влизане.

2. За да започнете унищожаването, щракнете или натиснете **Унищожаване**.

Избелване—Записва случайни данни на свободното пространство и предотвратява възстановяването на изтритите обекти.

▲ За да започнете избелването, щракнете или натиснете **Избелване**.

File Sanitizer опции—Изберете отметката, за да разрешите всяка от следните опции, или махнете отметката, за да забраните опция:

- **Разрешаване на икона на работен плот**—Показва иконата на File Sanitizer на работния плот на Windows.
- **Разрешаване на десен бутон**—Разрешава щракване с десен бутон или докосване и задържане върху актив, и после да изберете **HP File Sanitizer – Унищожаване**.
- **Искай парола за Windows преди ръчно унищожаване**—Изисква удостоверяване с парола за Windows преди ръчно унищожаване на обект.
- **Унищожаване на бисквитки и временни интернет файлове при затваряне на браузър**—Унищожава всички избрани уеб активи, като история на URL в браузъра, при затварянето на уеб браузъра.

Настройка на график за унищожаване

Можете да планирате време за автоматично унищожаване или да унищожавате активи ръчно по всяко време. За повече информация вижте Процедури за конфигуриране на страница 40.

1. Отворете File Sanitizer и щракнете или натиснете **Настройки**.
2. За да планирате бъдещо време за унищожаване на избрани активи, от **График за унищожаване** изберете **Никога**, **Еднократно**, **Ежедневно**, **Седмично** или **Месечно** и след това изберете ден и час:
   а. Щракнете или натиснете часа, минутата или полето AM/PM.
   б. Превъртете, докато желаната стойност се покаже на едно ниво с останалите полета.
   в. Щракнете или натиснете празното пространство до полетата за настройка.
   г. Повторете за всяко поле, докато изберете правилния график.
3. Изброени са следните четири вида активи:
   - **Кошче**—Унищожава всички обекти в кошчето.
   - **Временни системни файлове**—Унищожава всички файлове, намерени във временната системна папка. Търсят се следните променливи на средата в следния ред, и първият намерен път се приема за системна папка:
     - TMP
     - TEMP
   - **Временни интернет файлове**—Унищожава копия на уеб страници, изображения и мултимедия, записани от уеб браузърите за по-бързо преглеждане.
   - **Бисквитки**—Унищожава всички файлове, записани на компютъра от уеб сайтовете с цел запазване на предпочитанията, например информация за влизане.

   Ако са избрани, тези активи се унищожават в избраното време.
4. За да изберете допълнителни персонализирани активи за унищожаване:
   а. От **Списък за планирано унищожаване** щракнете или натиснете **Добавяне на папка** и се придвижете до файла или папката.
   б. Щракнете или натиснете **Отваряне**, после щракнете или натиснете **OK**.

   За да изтриете актив от Списъка за планирано унищожаване, махнете отметката от актива.

Настройка на график за избелване на свободното пространство

Избелването на свободното пространство не предоставя допълнителна защита на унищожените активи.

1. Отворете File Sanitizer и щракнете или натиснете **Настройки**.
2. За да планирате бъдещ момент за избелване на вашия твърд диск, в **График за избелване**, изберете **Никога**, **Веднъж**, **Дневно**, **Седмично** или **Месечно**, а след това изберете ден и час.
   a. Щракнете или натиснете часа, минутата или полето AM/PM.
   б. Превъртете, докато желаното време се покаже на едно ниво с останалите полета.
   в. Щракнете или натиснете празното пространство до полетата за настройка.
   г. Повторете, докато изберете правилния график.

ЗАБЕЛЕЖКА: Избелването на свободното пространство може да отнеме значително количество време. Уверете се, че компютърът е свързан към източник на променливотоково захранване. Макар че избелването на свободното пространство се изпълнява във фонов режим, увеличеното използване на процесора може да се отрази на работата на вашия компютър. Избелването на свободното пространство може да се изпълнява след работното време или когато компютърът не се използва.

Защита на файлове от унищожаване

За да защитите файлове или папки от унищожаване:

1. Отворете File Sanitizer и щракнете или натиснете **Настройки**.
2. От списъка **Никога не унищожавай** щракнете или натиснете **Добавяне на папка** и се придвижете до файла или папката.
3. Щракнете или натиснете **Отваряне**, после щракнете или натиснете **OK**.

ЗАБЕЛЕЖКА: Файловете в този списък са защитени дотогава, докато са в списъка.

За да изтриете актив от списъка с изключения, махнете отметката от актива.

Общи задачи

Използвайте File Sanitizer за изпълнение на следните задачи:

- **Използвайте иконата File Sanitizer за стартиране на унищожаване**—Влачете файловете до иконата **File Sanitizer** на работния плот на Windows. За подробности, вижте Използване на иконата File Sanitizer на страница 43.
- **Ръчно унищожаване на конкретен актив или на всички избрани активи**—Унищожавайте активите по всяко време, без да изчаквате планираното време за унищожаване. За подробности, вижте Унищожаване с десен бутон на страница 43 или Ръчно стартиране на унищожаване на страница 43.
- **Ръчно активиране на избелване на свободното пространство**—Активирайте избелване на свободното пространство по всяко време. За подробности, вижте Ръчно стартиране на избелване на свободното пространство на страница 44.
- **Преглед на регистрационни файлове**—Прегледайте регистрационните файлове от унищожаването и избелването на свободното пространство, които съдържат всички

грешки или неуспешни действия за последното унищожаване или избелване на свободното пространство. За подробности, вижте Преглед на регистрационни файлове на страница 44.

ЗАБЕЛЕЖКА: Унищожаването или избелването на свободното пространство може да отнеме значително количество време. Макар че унищожаването или избелването на свободното пространство се изпълняват във фонов режим, увеличеното използване на процесора може да се отрази на работата на вашия компютър.

Използване на иконата File Sanitizer

ВНИМАНИЕ: Унищожените активи не могат да бъдат възстановени. Внимателно обмислете кои елементи ще изберете за ръчно унищожаване.

Когато стартирате ръчно унищожаване, се унищожава стандартния списък за унищожаване в изгледа на File Sanitizer (вижте Процедури за конфигуриране на страница 40).

Можете да стартирате ръчно унищожаване по един от следните начини:

1. Отворете File Sanitizer (вижте Отваряне на File Sanitizer на страница 40) и щракнете или натиснете **Унищожаване**.
2. Когато се появи прозореца за потвърждение, уверете се, че активите, които желаете да унищожите са избрани, после щракнете или натиснете **OK**.

– или –

1. Щракнете с десен бутон или натиснете и задръжте иконата **File Sanitizer** на работния плот на Windows и щракнете или натиснете **Унищожаване сега**.
2. Когато се появи прозореца за потвърждение, уверете се, че активите, които желаете да унищожите са избрани, после щракнете или натиснете **Унищожаване**.

Унищожаване с десен бутон

ВНИМАНИЕ: Унищожените активи не могат да бъдат възстановени. Внимателно обмислете кои елементи ще изберете за ръчно унищожаване.

Ако е избрано **Разрешаване на унищожаване с десен бутон** в изгледа на File Sanitizer, можете да унищожите актив по следния начин:

1. Отидете до документа или папката, които искате да унищожите.
2. Щракнете с десен бутон или натиснете и задръжте файла или папката, после изберете **HP File Sanitizer – Унищожаване**.

Ръчно стартиране на унищожаване

ВНИМАНИЕ: Унищожените активи не могат да бъдат възстановени. Внимателно обмислете кои елементи ще изберете за ръчно унищожаване.

Когато стартирате ръчно унищожаване, се унищожава стандартния списък за унищожаване в изгледа на File Sanitizer (вижте Процедури за конфигуриране на страница 40).

Можете да стартирате ръчно унищожаване по един от следните начини:

1. Отворете File Sanitizer (вижте Отваряне на File Sanitizer на страница 40) и щракнете или натиснете **Унищожаване**.
2. Когато се появи прозореца за потвърждение, уверете се, че активите, които желаете да унищожите са избрани, после щракнете или натиснете **OK**.

– или –

1. Щракнете с десен бутон или натиснете и задръжте иконата **File Sanitizer** на работния плот на Windows и щракнете или натиснете **Унищожаване сега**.
2. Когато се появи прозореца за потвърждение, уверете се, че активите, които желаете да унищожите са избрани, после щракнете или натиснете **Унищожаване**.

Ръчно стартиране на избелване на свободното пространство

Когато стартирате ръчно избелване, се избелва стандартния списък за унищожаване в изгледа на File Sanitizer (вижте Процедури за конфигуриране на страница 40).

Можете да стартирате ръчно избелване по един от следните начини:

1. Отворете File Sanitizer (вижте Отваряне на File Sanitizer на страница 40) и щракнете или натиснете **Избелване**.
2. Когато се появи диалоговият прозорец за потвърждение, щракнете или натиснете **OK**.

– или –

1. Щракнете с десен бутон или натиснете и задръжте иконата **File Sanitizer** на работния плот на Windows и щракнете или натиснете **Избелване сега**.
2. Когато се появи диалоговият прозорец за потвърждение, щракнете или натиснете **Избелване**.

Преглед на регистрационни файлове

При всяко изпълнение на унищожаване или избелване, се генерират регистрационни файлове за грешки и неуспешни действия. Регистрационните файлове винаги се обновяват с последното унищожаване или избелване на свободното пространство.

ЗАБЕЛЕЖКА: Файловете, които са успешно унищожени или избелени, не се показват в регистрационните файлове.

Създава се един регистрационен файл за унищожаване и друг регистрационен файл за избелване на свободното пространство. И двата регистрационни файла се намират в следните папки на твърдия диск:

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

За 64-битови системи регистрационните файлове се намират в следните папки на твърдия диск:

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

7 HP Device Access Manager (само за избрани модели)

HP Device Access Manager управлява достъпа до данни, като забранява устройства за прехвърляне на данни.

ЗАБЕЛЕЖКА: Някои устройства за взаимодействие с човека/входни устройства, като например мишка, клавиатура, тъчпад и четец на пръстови отпечатъци, не се контролират от Device Access Manager. За повече информация вж. Класове устройства, които не се управляват на страница 49.

Администраторите на операционната система Windows® използват HP Device Access Manager, за да контролират достъпа на устройства до системата и да я защитават от неупълномощен достъп:

- Създават се профили на устройствата за всеки потребител, за да се определи за кои устройства има разрешение за достъп и за кои не.
- Just In Time Authentication (JITA) позволява на предварително определени потребители да се удостоверят, за да получат достъп до устройства, които по принцип за забранени.
- Администраторите и надеждните потребители могат да бъдат изключени от ограниченията за достъп на устройствата, наложени от Device Access Manager, като бъдат добавени към групата на администраторите на устройства. Членството в тази група се управлява с помощта на разширените настройки.
- Достъпът на устройствата може да се разрешава или забранява на базата на групово членство или за отделни потребители.
- За класове устройства като CD-ROM устройства може да се разреши или забрани поотделно достъпа за четене и достъпа за запис.

HP Device Access Manager се конфигурира автоматично със следните настройки по време на изпълнение на съветника за конфигуриране на HP Client Security:

- Сменяеми носители с Just In Time Authentication (JITA) са разрешени за групите Администратори и Потребители.
- Правилата за устройствата позволяват пълен достъп до други устройства.

Отваряне на Device Access Manager

1. От стартовия екран щракнете или натиснете приложението **HP Client Security** (Windows 8).

   – или –

   От работния плот на Windows щракнете двукратно или натиснете двукратно иконата **HP Client Security** в областта за уведомяване, разположена най-вдясно на лентата със задачи.

2. От **Устройство** щракнете или натиснете **Разрешения за устройства**.

   - Стандартните потребители могат да видят текущия си достъп до устройства (вижте Потребителски изглед на страница 46).
   - Администраторите могат да прегледат и направят промени в достъпа до устройствата, който е конфигуриран в момента за компютъра, като щракнат или натиснат **Промяна** и въведат администраторската парола (вижте Системен изглед на страница 46).

Потребителски изглед

Когато е избрано **Разрешения за устройства**, се показва потребителския изглед. В зависимост от правилата, стандартните потребители и администраторите могат да прегледат техния собствен достъп до класовете устройства или до отделни устройства на компютъра.

- **Текущ потребител**—Показва се името на потребителя, който е влязъл в момента.
- **Клас устройства**—Показва се вида на устройствата.
- **Достъп**—Показва се текущо конфигурираният достъп до видове устройства или конкретни устройства.
- **Продължителност**—Показва се времевото ограничение за достъп до CD/DVD-ROM устройства или сменяеми дискове.
- **Настройки**—Администраторите могат да променят достъпа до устройствата, който се управлява от Device Access Manager.

Системен изглед

В системния изглед администраторите могат да позволят или забранят достъп до устройства на този компютър за групите Потребители или Администратори.

▲ Администраторите имат достъп до системния изглед, като щракнат или натиснат **Промяна**, въведат администраторската парола и изберат някоя от следните опции:

- **Device Access Manager**—За да включите или изключите HP Device Access Manager с Just In Time Authentication, щракнете или натиснете **Включено** или **Изключено**.
- **Потребителите и групи на този компютър**—Показва групите Потребители или Администратори, на които са забранени или разрешени избраните класове устройства.
- **Клас устройства**—Показва класовете устройства и устройствата, които са инсталирани в системата или които може да са били инсталирани преди това в системата. За да отворите списъка, щракнете върху иконата **+**. Показани са всички устройства, свързани към компютъра, а групите Администратори и Потребители са разтворени, за да се видят

членовете им. За да обновите списъка с устройства, щракнете върху иконата с кръгла стрелка (обновяване).

- Защитата обикновено се прилага върху клас устройства. Ако достъпът е конфигуриран като **Разрешен**, избраният потребител или група имат достъп до всяко устройство в класа устройства.
- Защитата може да се приложи и за конкретни устройства.
- Конфигурирайте Just In Time authentication (JITA), което позволява на избраните потребители достъп до DVD/CD-ROM устройства или сменяеми дискове, след като се удостоверят. За повече информация вж. Конфигуриране на JITA на страница 48.
- Разрешете или забранете достъп до други класове устройства, например сменяеми носители (като USB флаш устройства), серийни и паралелни портове, Bluetooth® устройства, модеми, PCMCIA/ExpressCard устройства, 1394 устройства, четец на пръстови отпечатъци и четец за смарт карти. Ако са забранени четец на пръстови отпечатъци и четец за смарт карти, те могат да се използват за идентификационни данни за удостоверяване, но не могат да се използват на ниво сесия според правилата.

  ЗАБЕЛЕЖКА: Ако се използват Bluetooth устройства за идентификационни данни за удостоверяване, достъпът до Bluetooth устройствата не трябва да е ограничен в правилата на Device Access Manager.

- Когато изберете настройка на ниво Група или Клас устройства, и трябва да изберете дали да приложите тази настройка за подчинените обекти:

  Да—Настройката ще се приложи надолу.

  Не—Настройката няма да се приложи надолу.

- Някои класове устройства, например DVD и CD-ROM, може да се управляват освен това чрез отделно разрешаване или забраняване на достъп за операции за четене или писане.

  ЗАБЕЛЕЖКА: Групата Администратори не може да се добавя към списъка с потребители.

- **Достъп**—Щракнете или натиснете стрелката надолу, после изберете един от следните типове достъп, за да го разрешите или забраните:
  - **Разрешен – Пълен достъп**
  - **Разрешен – Само за четене**
  - **Разрешен – Изисква се JITA**—За повече информация, вижте Конфигуриране на JITA на страница 48.

    Ако е избран този вид достъп, от **Продължителност** щракнете или натиснете стрелката надолу, за да изберете времево ограничение.
  - **Забранен**
- **Продължителност**—Щракнете или натиснете стрелката надолу, за да изберете времево ограничение за достъп до CD/DVD-ROM устройства или сменяеми дискове (вижте Конфигуриране на JITA на страница 48).

Конфигуриране на JITA

Конфигурирането на JITA позволява на администратора да прегледа и промени списъка с потребители и групи, които имат позволен достъп до устройства чрез използване на Just In Time Authentication (JITA).

Потребителите с разрешен JITA ще имат достъп до някои устройства, за които са създадени правила за ограничение в **Конфигурация на класове устройства**.

Периодът за JITA може да бъде разрешен за зададен брой минути или да е неограничен. Потребителите с неограничено време за достъп ще имат достъп до устройството от момента, в който се удостоверят, докато излязат от системата.

Ако на потребител е зададен ограничен период за JITA, една минута преди изтичане на периода за JITA потребителят ще бъде попитан дали да увеличи времето за достъп. Веднага, щом потребителят излезе от системата или друг потребител влезе, периодът за JITA изтича. При следващото влизане на потребителя и опит за достъп до устройство с JITA, се появява прозорец за въвеждане на идентификационни данни.

JITA е наличен за следните класове устройства:

- DVD/CD-ROM устройства
- Сменяеми дискове

Създаване на правила за JITA за потребител или група

Администраторите могат да разрешат на потребители и групи достъп до устройства с използване на Just In Time Authentication (JITA).

1. Стартирайте **Device Access Manager** и щракнете или натиснете **Промяна**.
2. Изберете потребителя или групата, после от **Достъп** за **Сменяеми дискове** или за **DVD/CD-ROM устройства** щракнете или натиснете стрелка надолу, после изберете **Разрешен – Изисква се JITA**.
3. От **Продължителност** щракнете или натиснете стрелката надолу, за да изберете периода от време за JITA достъп.

Потребителят трябва да излезе и да влезе отново, за да се приложат новите настройки за JITA.

Правила за забрана на JITA за потребител или група

Администраторите могат да забранят на потребител и група достъп до устройства с използване на Just In Time Authentication.

1. Стартирайте **Device Access Manager** и щракнете или натиснете **Промяна**.
2. Изберете потребителя или групата, после от **Достъп** за **Сменяеми дискове** или за **DVD/CD-ROM устройства** щракнете или натиснете стрелка надолу, после изберете **Забранен**.

Когато потребителят влезе и се опита да достъпи устройството, достъпът е забранен.

Настройки

Изгледът **Настройки** позволява на администраторите да прегледат и променят достъпа до устройствата, който се управлява от Device Access Manager.

ЗАБЕЛЕЖКА: Device Access Manager трябва да е разрешен при конфигуриране на списъка с буквите на дисковете (вижте Системен изглед на страница 46).

Класове устройства, които не се управляват

HP Device Access Manager не управлява следните класове устройства:

- Входни/изходни устройства
  - CD-ROM
  - Дисково устройство
  - Флопи дисково устройство (FDC)
  - Контролер за твърд диск (HDC)
  - Клас интерфейсни устройства (HID)
  - Инфрачервени интерфейсни устройства
  - Мишка
  - Мини-сериен порт
  - Клавиатура
  - Plug and play (PnP) принтери
  - Принтер
  - Надстройка на принтер
- захранване
  - Поддръжка на разширено управление на захранването (APM)
  - Батерия
- Разни
  - Компютър
  - Декодер
  - Дисплей
  - Универсален драйвер за дисплей Intel®
  - Legacard
  - Медия драйвер
  - Устройство за смяна на носител
  - Технологии за памет
  - Монитор
  - Многофункционални
  - Net client
  - Net service
  - Net trans

- Процесор
- SCSI адаптер
- Акселератор за защита
- Устройства за защита
- Система
- Неизвестно
- Том
- Моментна снимка на том

8 HP Trust Circles

HP Trust Circles е приложение за защита на файлове и документи, което комбинира шифроване на файлове в папка с удобна възможност за споделяне на документи в trust circle. Приложението шифрова файловете, поставени в зададени от потребителя папки, като ги защитава в trust circle. След като са защитени, файловете могат да се използват и споделят само от членове на trust circle. Ако защитеният файл бъде получен от потребител, който не е член на trust circle, файлът остава шифрован и този потребител няма достъп до съдържанието.

Отваряне на Trust Circles

1. От стартовия екран щракнете или натиснете приложението **HP Client Security**.

   – или –

   От работния плот на Windows щракнете двукратно върху иконата **HP Client Security** в областта за уведомяване, разположена най-вдясно на лентата със задачи.

2. От **Данни** щракнете или натиснете **Trust Circles**.

Първи стъпки

Има два начина да изпратите покани по имейл и да им отговорите:

- **Като използвате Microsoft® Outlook**—Използването на Trust Circles с Microsoft Outlook автоматизира обработката на Trust Circle поканите и отговорите от други потребители на Trust Circle.
- **Като използвате Gmail, Yahoo, Outlook.com или други имейл услуги (SMTP)**—Когато въведете вашето име, имейл адрес и парола, Trust Circles използва вашата имейл услуга за изпращане на покани по имейл до членовете, избрани да се включат във вашия trust circle.

За да настроите вашия основен профил:

1. Въведете вашето име и имейл адрес, после щракнете или натиснете **Напред**.

   Името се вижда от всички членове, които поканите да се включат във вашия trust circle. Имейл адресът се използва за изпращане, получаване или отговор на покани.

2. Въведете паролата за вашия имейл акаунт, после щракнете или натиснете **Напред**.

   Изпраща се тестов имейл, за да е сигурно, че настройките на имейла са правилни.

   ЗАБЕЛЕЖКА: Компютърът трябва да е свързан към мрежа.

3. В полето **Trust Circle Name** (име на trust circle) въведете името на trust circle,а след това щракнете или натиснете **Напред**.

4. Добавете членове и папки, после щракнете или натиснете **Напред**. Trust circle се създава с всички избрани папки и изпраща покани по имейл на всички избрани членове. Ако по някаква причина не може да се изпрати покана, се показва съобщение. Членовете могат да бъдат поканени по всяко време от изгледа Trust Circle, като щракнете върху **Your Trust**

Circles (Вашите Trust Circles), а след това щракнете двукратно или натиснете двукратно върху trust circle. За повече информация вж. Trust Circles на страница 52.

Trust Circles

Можете да създадете trust circle по време на първоначалната настройка след като въведете имейл адрес или от изгледа Trust Circle:

▲ От изгледа Trust Circle щракнете или натиснете **Create Trust Circle** (Създаване на trust circle), а след това въведете име за trust circle.

- За да добавите членове към trust circle, щракнете или натиснете иконата **M+** до **Members** (членове), а след това следвайте указанията на екрана.
- За да добавите папки към trust circle, щракнете или натиснете иконата **+** до **Folders** (Папки), а след това следвайте указанията на екрана.

Добавяне на папки към trust circle

Добавяне на папки към нов trust circle:

- При създаването на trust circle, можете да добавите папки, като щракнете или натиснете иконата **+** до **Folders** (Папки), а след това следвате указанията на екрана.

  – или –

- В Windows Explorer щракнете с десен бутон или натиснете и задръжте върху папката, която в момента не е част от trust circle, изберете **Trust Circle**, а след това изберете **Create Trust Circle from Folder** (Създаване на trust circle от папка).

СЪВЕТ: Можете да изберете една или повече папки.

Добавяне на папки към съществуващ trust circle:

- От изгледа Trust Circle щракнете върху **Your Trust Circles** (Вашите trust circles), щракнете двукратно или натиснете двукратно върху съществуващ trust circle, за да се покажат текущите папки, щракнете или натиснете иконата **+** до **Folders** (Папки), а след това следвайте указанията на екрана.

  – или –

- В Windows Explorer щракнете с десен бутон или натиснете и задръжте върху папката, която в момента не е част от trust circle, изберете **Trust Circle**, после изберете **Add to existing Trust Circle from Folder** (Добавяне към съществуващ trust circle от папка).

СЪВЕТ: Можете да изберете една или повече папки.

След като папката е добавена към trust circle, Trust Circles автоматично шифрова папката и нейното съдържание. След като всички файлове са шифровани, се показва съобщение. Освен това се показва зелен катинар на всички икони на шифровани папки и файлове в папките, който показва, че те са напълно защитени.

Добавяне на членове към trust circle

Необходими са три стъпки за добавяне на членове към trust circle:

1. **Покана**—Първо, собственикът на trust circle кани члена(овете). Имейлът с поканата може да бъде изпратен на множество потребители или списъци/групи за разпространение.
2. **Приемане**—Поканеният получава поканата и решава дали да я приеме или отхвърли. Ако поканеният приеме поканата, на поканилия се изпраща имейл в отговор. Ако поканата е изпратена на група, всеки член получава покана и решава дали да я приеме или отхвърли.
3. **Регистриране**—Канещият има окончателна възможност да реши дали да добави член към trust circle. Ако канещият реши да регистрира члена, на поканения се изпраща имейл за потвърждение на отговора на поканата. Канещият и поканеният могат освен това да проверят защитата на процеса на покана. На поканения се показва код за потвърждение, който трябва да бъде прочетен на канещия по телефона. След като кодът бъде потвърден, канещият може да изпрати окончателния имейл за регистрация.

Добавяне на членове към нов trust circle:

▲ При създаването на trust circle можете да добавите членове, като щракнете или натиснете иконата **M+** до **Members** (Членове), а след това следвате указанията на екрана.

- Ако използвате Outlook, изберете контакти от адресната книга на Outlook, после щракнете върху **OK**
- Ако използвате друга имейл услуга, добавете ръчно новите имейл адреси към Trust Circle, или можете да ги вземете от имейл адресите, регистрирани в Trust Circle.

Добавяне на членове към съществуващ trust circle:

▲ От изгледа Trust Circle щракнете върху **Your Trust Circles** (Вашите trust circles), щракнете двукратно или натиснете двукратно върху съществуващ trust circle, за да се покажат текущите членове, щракнете или натиснете иконата **M+** до **Members** (Членове), а след това следвайте указанията на екрана.

- Ако използвате Outlook, изберете контакти от адресната книга на Outlook, после щракнете върху **OK**.
- Ако използвате друга имейл услуга, добавете ръчно новите имейл адреси към Trust Circle, или можете да ги вземете от имейл адресите, регистрирани в Trust Circle.

Добавяне на файлове към trust circle

Можете да добавите файлове към trust circle по един от следните начини:

- Копирайте или преместете файла в съществуваща папка в trust circle.

  – или –

- В Windows Explorer, щракнете с десен бутон или натиснете и задръжте файл, който в момента не е шифрован, изберете **Trust Circle**, а след това изберете **Encrypt**. Ще трябва да изберете trust circle, към който да добавите файла.

СЪВЕТ: Можете да изберете един или повече файлове.

Шифровани папки

Всеки член на trust circle може да преглежда и редактира файлове, които принадлежат на този trust circle.

ЗАБЕЛЕЖКА: Trust Circle Manager/Reader не синхронизира файловете между членовете.

Файловете трябва да се споделят по съществуващите начини, например имейл, ftp или доставчици на облачни услуги. Файловете, които са копирани, преместени или създадени в trust circle, са незабавно защитени.

Премахване на папки от trust circle

Премахването на папка от trust circle дешифрира папката и цялото ѝ съдържание и премахва защитата им.

- От изгледа Trust Circle щракнете или натиснете **Your Trust Circles**, щракнете двукратно или натиснете двукратно върху съществуващ trust circle, за да се покажат текущите папки, щракнете или натиснете иконата **кошче** до папката.

  – или –

- В Windows Explorer щракнете с десен бутон или натиснете и задръжте върху папката, която в момента е част от trust circle, изберете **Trust Circle**, после изберете **Remove from trust circle**.

СЪВЕТ: Можете да изберете една или повече папки.

Премахване на файл от trust circle

За да премахнете файл от trust circle, в Windows Explorer, щракнете с десен бутон или натиснете и задръжте върху файл, който в момента не е шифрован, изберете **Trust Circle**, изберете **Decrypt File**.

Премахване на членове от trust circle

Член, който е регистриран докрай, не може да бъде премахнат от trust circle. Алтернативна възможност е да се създаде нов trust circle с всички останали членове, да се преместят всички файлове и папки в новия trust circle, а след това и да се изтрие старият trust circle. Това гарантира, че всички нови файлове, които получи този член, няма да са достъпни, но всичко, което е било споделено преди това, ще остане достъпно за члена на стария trust circle.

Ако даден член не е регистриран докрай (или е бил поканен да се включи в trust circle, или не е приел поканата за trust circle), можете да премахнете члена от trust circle по един от следните начини:

- От изгледа Trust Circle щракнете или докоснете **Your Trust Circles** (Вашите Trust Circles), а след това щракнете двукратно или натиснете двукратно trust circle, за да се покаже текущият списък с членове. Щракнете или натиснете иконата на **кошчето** до името на члена, който искате да премахнете.
- От изгледа Trust Circle щракнете или докоснете **Members** (Членове), после щракнете двукратно или натиснете двукратно члена, за да се покажат trust circles, на които е член. Щракнете или натиснете иконата на **кошчето** до trust circle, за да премахнете члена от този trust circle.

Изтриване на trust circle

За да изтриете trust circle, е необходимо да сте собственик.

▲ От изгледа Trust Circle щракнете или натиснете **Your Trust Circles** (Вашите Trust Circles) и щракнете или натиснете иконата на **кошчето** до trust circle, който искате да изтриете.

Това премахва trust circle от страницата и изпраща имейли на всички членове на този trust circle , за да ги информира, че даденият trust circle е изтрит. Всички файлове и папки, които са били включени в този trust circle, се дешифрират.

Задаване на предпочитания

От изгледа Trust Circle щракнете или натиснете **Предпочитания**. Показват се три раздела

- **Настройки на имейл**

Опция	Описание
Username (Потребителско име)	Показва се използваното в момента потребителско име. За да го промените, въведете ново потребителско име в текстовото поле. Промените се записват автоматично.
Email Address (Имейл адрес)	Показва се използваният в момента имейл адрес. За да го промените, щракнете или натиснете **Change Email Settings** (Промяна на настройки на имейл) и следвайте указанията на екрана.
New Member Confirmation (Потвърждение за нов член)	Изберете между следните опции: ◦ **Confirm Automatically** (Автоматично потвърждение)—След получаване на приетата покана от поканения(те), те се потвърждават в trust circle без никакво ръчно въвеждане и се изпраща имейл за потвърждение към поканения(те). ◦ **Confirm Manually** (Ръчно потвърждение)—След получаване на приетата покана от поканения(те), е необходимо ръчно въвеждане за регистриране на новите членове в trust circle и се изпраща имейл за потвърждение към поканения(те). ◦ **Require Verification** (Изисква се проверка)—След получаване на приетата покана от поканения(те), се изисква код за потвърждение за регистриране докрай на поканения(те). Собственикът на доверения кръг трябва да се свърже с поканения(те) и да получи кода за потвърждение от тях. След въвеждане на правилния код, се изпращат имейли за потвърждение.
Periodic Authentication (Периодично удостоверяване)	Периодичното удостоверяване изисква потребителят да въведе парола за Windows след указан период от време на изчакване (записано в минути), както и при изпълнение на чувствителни операции. Тази настройка позволява на потребителите да включват или изключват удостоверяването.
Authentication Timeout (Време на изчакване за удостоверяване)	Изберете зададеният период на изчакване (записан в минути) преди да се изисква удостоверяване.

Опция	Описание
Don't show confirmation message (Не показвай съобщение за потвърждение)	Изберете отметката, за да забраните показването на съобщения за потвърждение, или махнете отметката, за да се показват.
I'd like to help improve the HP Trust Circle through anonymous usage tracking (Искам да помогна за подобряването на HP Trust Circle чрез анонимно наблюдение на използването)	Изберете отметката, за да участвате в програмата или махнете отметката, ако не желаете да участвате.

- **Backup/Restore** (Архивиране/Възстановяване)

Опция	Описание
Архивиране	Копира данните от приложението Trust Circle Manager/Reader (настройки и доверени кръгове) в архивен файл. В случай на срив или отказ на системата, можете да използвате този файл, за да възстановите вашата нова инсталация на Trust Circles до състоянието, записано във файла. **ЗАБЕЛЕЖКА:** Записват се само данните за приложението Trust Circle (доверени кръгове, настройки и членове). Действителните файлове в папките на доверените кръгове не се архивират. Тези файлове трябва да се архивират отделно. За да архивирате настройките на Trust Circle и потребителските данни: **1.** Щракнете или натиснете **Архивиране**. **2.** Изберете име на файл и папка за архивния файл, после щракнете или натиснете **Запис**. **3.** Въведете парола, потвърдете я, после щракнете или натиснете **OK**. Тази парола ще се изисква при възстановяване на файла.
Възстановяване	Възстановява настройките и доверените кръгове от архивен файл, обикновено след срив на системата или миграция на друг компютър. За да възстановите настройките и потребителските данни на Trust Circle Manager: **1.** Щракнете или натиснете **Restore** (Възстановяване). **2.** Отидете до папката и името на файла в архивния файл, после щракнете или натиснете **Open** (Отваряне). **3.** Въведете паролата, която е била настроена при създаването на архива.

- **About** (За)—Показва се версията на софтуера Trust Circle Manager/Reader. Показват се връзки, които ви позволяват да обновите Trust Circle Manager до версия Pro или се показва Декларацията за поверителност на HP.

9 Възстановяване след кражба (само при някои модели)

Computrace (закупува се отделно) ви позволява дистанционно да наблюдавате, управляваье и проследявате вашия компютър.

След активиране Computrace се конфигурира от центъра за обслужване на клиенти Absolute Software. От центъра за обслужване на клиенти администраторът може да конфигурира Computrace да извършва наблюдение или управление на компютъра. Ако системата се изгуби или бъде откраднатa, центърът за обслужване на клиенти може да съдейства на местните власти при откриването и възстановяването на компютъра. Ако се конфигурира, Computrace може да продължи да функционира, дори ако твърдият диск бъде изтрит или сменен.

За да активирате Computrace:

1. Свържете се сИнтернет.
2. Отворете HP Client Security. За повече информация вж. Отваряне на HP Client Security на страница 10.
3. Щракнете върху **Theft Recovery** (Възстановяване след кражба).
4. За да стартирате съветника за активиране на Computrace, щракнете върху **Get Started** (Начални стъпки).
5. Въведете вашата информация за контакт и информация за плащане с кредитна карта или въведете предварително закупен продуктов ключ.

Съветникът за активиране безопасно обработва транзакцията и конфигурира вашия потребителски акаунт на уебсайта на центъра за обслужване на клиенти Absolute Software. След завършване на транзакцията ще получите имейл за потвърждение, който съдържа информация за вашия акаунт в центъра за обслужване на клиенти.

Ако преди това сте използвали съветника за активиране на Computrace и вече имате съществуващ потребителски акаунт, можете да закупите допълнителни лицензи, като се свържете с вашия представител на HP.

За да влезете в центъра за обслужване на клиенти:

1. Отидете на https://cc.absolute.com/.
2. В полетата **Login ID** и **Password** въведете идентификационните данни, които сте получили в имейла за потвърждение, а след това щракнете върху **Log in**.

С помощта на центъра за обслужване на клиенти вие можете:

- Да наблюдавате компютрите си.
- Да защитавате дистанционните си данни.
- Да докладвате за кражбата на който и да е компютър, защитен от Computrace.

▲ Щракнете върху **Learn More** за повече информация относно Computrace.

10 Изключения за локализирани пароли

На ниво Удостоверяване при включване и на ниво HP Drive Encryption поддръжката за локализирани пароли е ограничена. За повече информация вж. Windows IME, които не се поддържат на ниво Удостоверяване при включване или на ниво Drive Encryption на страница 58.

Какво да направим, когато паролата е отхвърлена

Паролите могат да бъдат отхвърлени по следните причини:

- Потребител използва IME, който не се поддържа. Това е чест проблем при езици с двойни байтове (корейски, японски, китайски). За решаване на проблема:

  1. Като използвате **контролен панел** добавете поддържана клавиатурна подредба (добавете US/English клавиатури за китайски език на въвеждане).
  2. Настройте поддържаните клавиатури за въвеждане по подразбиране.
  3. Стартирайте HP Client Security, после въведете паролата за Windows.

- Потребител използва символ, който не се поддържа. За решаване на проблема:

  1. Сменете паролата за Windows, за да използва само поддържани символи. За повече информация за неподдържаните символи, вижте Работа със специални клавиши на страница 59.
  2. Стартирайте HP Client Security, после въведете паролата за Windows.

Windows IME, които не се поддържат на ниво Удостоверяване при включване или на ниво Drive Encryption

В Windows потребителят може да избере IME (редактор за начин на въвеждане), за да въведе сложни символи, например японски или китайски символи, като използва стандартна западна клавиатура.

IME не се поддържат на ниво Удостоверяване при включване или на ниво Drive Encryption. Паролата за Windows не може да бъде въведена с IME в екрана за влизане за Удостоверяване при включване или HP Drive Encryption и това може да доведе до заключване. В някои случаи Microsoft® Windows не показва IME, когато потребителят въвежда паролата.

Решението е да се превключи на една от следните клавиатурни подредби, които превеждат до клавиатурна подредба 00000411:

- Microsoft IME за японски
- Японска клавиатурна подредба
- Office 2007 IME за японски—Ако Microsoft или трета страна използва термина IME или редактор за начин на въвеждане, начинът за въвеждане може всъщност да не е IME. Това предизвиква объркване, но софтуерът чете представянето в шестнадесетичен вид. Така,

ако IME е свързан към поддържана клавиатурна подредба, HP Client Security може да поддържа конфигурацията.

ПРЕДУПРЕЖДЕНИЕ! Когато се внедрява HP Client Security, въведените пароли с Windows IME ще бъдат отхвърлени.

Смяна на парола с клавиатурни подредби, които също се поддържат

Ако паролата е била първоначално зададена с една клавиатурна подредба, например U.S. English (409), а после потребителят смени паролата, като използва друга клавиатурна подредба, която също се поддържа, например Latin American (080A), смяната на паролата ще работи в HP Drive Encryption, но няма да работи в BIOS, ако потребителят използва символи, които съществуват във втората, но не и в първата (например ē).

ЗАБЕЛЕЖКА: Администраторите могат да разрешат този проблем, като използват страницата Потребители в HP Client Security (достъпна от иконата **Gear** (настройки) в началната страница), за да премахнат потребителя от HP Client Security, да изберат желаната клавиатурна подредба в операционната система, после да стартират съветника за конфигуриране на HP Client Security отново за същия потребител. BIOS записва желаната клавиатурна подредба и паролите, които могат да се въведат с тази клавиатурна подредба ще бъдат правилно зададени в BIOS.

Друг възможен проблем е използването на различни клавиатурни подредби, които могат да възпроизвеждат еднакви символи. Например клавиатурна подредба U.S. International (20409) и клавиатурна подредба Latin American (080A) могат да възпроизвеждат символа é, макар че се изисква различна последователност от клавиши. Ако паролата е първоначално зададена с клавиатурна подредба Latin American, то в BIOS е зададена клавиатурната подредба Latin American, дори ако паролата после е сменена с клавиатурна подредба U.S. International.

Работа със специални клавиши

- Китайски, словашки, френски канадски и чешки

  Когато даден потребител избере една от горепосочените клавиатурни подредби и въведе парола (например, abcdef), същата парола трябва да се въведе, като се натиска клавиша shift за малки букви и клавишите shift и caps lock за главни букви при удостоверяване при включване и HP Drive Encryption. Паролите с цифри трябва да се въвеждат чрез използване на цифровата клавиатура.

- Корейски

  Когато даден потребител избере една от поддържаните корейски клавиатурни подредби и въведе парола, същата парола трябва да се въведе, като се натиска десния клавиш alt за малки букви и десния клавиш alt и клавиша caps lock за главни букви при удостоверяване при включване и HP Drive Encryption.

- Неподдържаните символи са изброени в следната таблица:

Language (Език)	Windows	BIOS	Drive Encryption
Арабски	Клавишите ﻻ, ﻷ и ﻹ генерират два символа.	Клавишите ﻻ, ﻷ и ﻹ генерират един символ.	Клавишите ﻻ, ﻷ и ﻹ генерират един символ.

Language (Език)	Windows	BIOS	Drive Encryption
Френски канадски	ç, è, à, и é с caps lock са Ç, È, À, и É в Windows.	ç, è, à, и é с caps lock са ç, è, à, and é при удостоверяване при включване.	ç, è, à, и é с caps lock са ç, è, à, и é при HP Drive Encryption.
Испански	40a не се поддържа. Но въпреки това работи, защото софтуерът го конвертира в c0a. Но поради леката разлика между клавиатурните подредби се препоръчва испано-говорящите потребители да сменят клавиатурната си подредба за Windows на 1040a (Spanish Variation) или 080a (Latin American).	няма информация	няма информация
US international	◦ Клавишите ¡, ¤, ‘, ’, ¥ и × на горния ред се отхвърлят. ◦ Клавишите å, ® и Þ на втория ред се отхвърлят. ◦ Клавишите á, ð и ø на третия ред се отхвърлят. ◦ Клавишът æ на последния ред се отхвърля.	няма информация	няма информация
Чешки	◦ Клавишът ğ се отхвърля. ◦ Клавишът į се отхвърля. ◦ Клавишът ų се отхвърля. ◦ Клавишите ė, ı и ż се отхвърлят. ◦ Клавишите ģ, ķ, ļ, ņ и ţ се отхвърлят.	няма информация	няма информация
Словашки	Клавишът ż се отхвърля.	◦ Клавишите š, ś и ş се отхвърлят при въвеждане, но се приемат при въвеждане от софтуерна клавиатура. ◦ Пасивният клавиш ţ генерира два символа.	няма информация
Унгарски	Клавишът ż се отхвърля.	Клавишът ţ генерира два символа.	няма информация

Language (Език)	Windows	BIOS	Drive Encryption
Словенски	Клавишът żŻ се отхвърля от Windows, а клавишът alt генерира пасивен клавиш в BIOS.	ú, Ú, ů, Ů, ş, Ş, ś, Ś, š и Š се отхвърлят в BIOS.	няма информация
Японски	Когато има, Microsoft Office 2007 IME е по-добрият избор. Въпреки името IME, това всъщност е клавиатурна подредба 411, която се поддържа.	няма информация	няма информация

Терминологичен речник

Bluetooth
Технология, която използва радио предаване, за да позволи на Bluetooth компютри, принтери, мишки, мобилни телефони и други устройства безжична комуникация на къси разстояния.

Drive Encryption
Защитава данните ви, като шифрова вашия(те) твърд(и) диск(ове) и по този начин информацията не може да се чете от неупълномощени лица.

DriveLock
Функция за защита, която свързва твърдия диск с потребител и изисква потребителят да въведе правилно паролата за DriveLock при стартиране на компютъра.

ID карта
Притурка за работния плот на Windows, която служи за визуално идентифициране на вашия работел плот с вашето потребителско име и избрана снимка.

Just In Time Authentication
Вижте Помощ в софтуера HP Device Access Manager.

PIN
Персонален идентификационен номер за регистриран потребител, който се използва за удостоверяване.

PKI
Стандартът за Инфраструктура за публични ключове, който определя интерфейса за създаване, употреба и управление на сертификати и криптографски ключове.

Trust Circle
Предоставя защита на данните чрез обвързването им в определена група от надеждни потребители. Това предотвратява случайно или умишлено попадане на данните в погрешни ръце. Защитени с технологията CryptoMill's Zero Overhead Key Management, данните са криптографски обвързани в кръг на доверие. Това предотвратява дешифриране на документи или друга поверителна информация извън trust circle.

Trust Circle Manager/Reader
Trust Circle Reader може само да приема покани, изпратени от потребителите на Trust Circle Manager. Но Trust Circle Manager позволява създаването на доверени кръгове. Функциите включват покана към някого в доверен кръг по имейл и приемане на поканите за доверен кръг от други. След установяване на доверен кръг между партньорите, файловете, защитени в този доверен кръг, може да се споделят безопасно.

Trusted Platform Module (TPM) - чип за вградена защита
TPM удостоверява по-скоро даден компютър, отколкото потребител, като съхранява специфична информация за системата на хоста, като например ключове за шифроване, цифрови сертификати и пароли. TPM намалява до мнимум риска за компреметиране на информацията на компютъра чрез физическа кражба или атака от външен хакер.

автоматично унищожаване
Унищожаване, което вие планирате във File Sanitizer.

администратор
Вижте *администратор на Windows*.

Администратор на Windows

Потребител с пълни права за промяна на права и управление на други потребители.

актив
Компонент от данни, който се състои от лична информация или файлове, исторически и уеб данни и т.н., който се намира на твърдия диск.

активиране
Задача, която трябва да бъде изпълнена, за да станат достъпни функциите на Drive Encryption. Администраторите могат да активират Drive Encryption със съветника за конфигуриране на HP Client Security или с HP Client Security. Процесът на активация се състои от активиране на софтуера, шифроване на диска и създаване на първоначален резервен ключ на сменяемо устройство за съхраняване на данни.

архив
Използване на функция за архивиране за записване на копие на важна програмна информация на място извън програмата. След това то може да се използва за възстановяване на информацията по-късно на същия компютър или на друг.

архив за аварийно възстановяване
Защитена област за съхранение, която позволява повторно шифроване на клавишите на основен потребител при смяна на платформата.

безконтактна карта
Пластмасова карта, съдържаща компютърен чип, която може да се използва за удостоверяване.

влизане
Обект в рамките на HP Client Security, който включва потребителско име и парола (възможно е да включва и друга избрана информация), и може да се използва за влизане в уебсайтове или други програми.

възстановяване
Процес, който копира програмна информация от запазен предишен архивен файл в тази програма.

Възстановяване с HP SpareKey
Възможността за осъществяване на достъп до вашия компютър след даване на правилен отговор на въпроси за защита.

група
Група от потребители, които имат еднакво ниво на разрешен или забранен достъп до клас устройства или конкретно устройство.

дешифриране
Процедура, използвана в криптографията за превръщане на шифровани данни в обикновен текст.

домейн
Група от компютри, които са част от мрежа и споделят обща директория с база данни. Домейните са с уникални имена и всеки има набор от общи правила и процедури.

Еднократна идентификация
Функция, която съхранява информация за удостоверяване и ви позволява да използвате HP Client Security за достъп до приложения в Интернет и Windows, които изискват удостоверяване с парола.

Екран за влизане в Drive Encryption
Вижте Удостоверяване преди зареждане през Drive Encryption.

Защита при влизане в Windows
Защитава вашият(те) акаунт(и) в Windows, като изисква използване на специфични идентификационни данни за достъп.

идентификационни данни

Конкретна информация или хардуерно устройство, използвани за удостоверяване на отделен потребител.

избелване на свободното пространство
Записването на случайни данни върху изтрити активи и неизползвано пространство. Този процес намалява съществуването на изтрития актив така, че оригиналният актив е по-труден за възстановяване.

карта с чип
Пластмасова карта, съдържаща компютърен чип, която може да се използва за удостоверяване в комбинация с други идентификационни данни за допълнителна защита.

клас устройства
Всички устройства от определен вид, например дискове.

метод за защитено влизане
Методът, използван за влизане в компютъра.

мрежов акаунт
Потребителски или администраторски акаунт в Windows на локален компютър, в работна група или в домейн.

Начална страница
Централно място, от където имате достъп и управлявате функциите и настройките на HP Client Security.

Папка от Trust Circle
Всяка папка, защитена от trust circle.

политика за контрол на достъпа на устройствата
Списък от устройства, за които на потребителя е разрешен или забранен достъпа.

потребител
Всеки, регистриран в Drive Encryption. Потребителите, които не са администратори, имат ограничени права в Drive Encryption. Те могат само да се регистрират (с одобрение на администратора) и да влязат.

Потребителски акаунт в Windows
Потребител, който има право да влиза в мрежата или на отделен компютър.

Принудително предстартово удостоверяване на Drive Encryption
Екран за влизане, който се показва преди стартирането на Windows. Потребителите трябва да въведат потребителското си име и парола за Windows или PIN код на смарт карта, или да плъзнат регистриран пръст. Ако бъде избрано влизане с едно действие, въвеждането на правилната информация в екрана за влизане на Drive Encryption позволява директен достъп до Windows, без да се влиза отново в екрана за влизане на Windows.

пръстов отпечатък
Цифрово извличане на изображение на вашия пръстов отпечатък. Вашето действително изображение на пръстов отпечатък никога не се съхранява в HP Client Security.

рестартиране
Процесът на рестартиране на компютъра.

ръчно унищожаване
Незабавно унищожаване на актив или избрани активи, който заобикаля планираното унищожаване.

самоличност
В HP Client Security, група от идентификационни данни и настройки, които се управляват като акаунт или профил за определен потребител.

свързано устройство
Хардуерно устройство, което е свързано към порт в компютъра.

смарт карта
Хардуерно устройство, което може да се използва с PIN код за удостоверяване.

софтуерно шифроване
Използването на софтуер за шифроване на твърдия диск сектор по сектор. Този процес е по-бавен от хардуерно шифроване

удостоверяване
Процесът на удостоверяване дали вие сте лицето, за което се представяте, като се използват идентификационни данни, включително парола за Windows, пръстови отпечатъци, смарт карта, безконтактна карта или карта с чип.

удостоверяване при включване
Функция за защита, която изисква някаква форма на удостоверяване, като например смарт карта, чип за защита или парола при включване на компютъра.

унищожаване
Изпълнение на алгоритъм, който презаписва данните, съдържащи се в актив, с безсмислени данни.

Файлова система за шифроване (EFS)
Система, която шифрова всички файлове и подпапки в избрана папка.

хардуерно шифроване
Използването на дискове за самостоятелно шифроване, които отговарят на спецификацията на Trusted Computing Group OPAL за управление на дискове със самостоятелно шифроване за изпълнение на моментално шифроване. Хардуерното шифроване е моментално и може да отнеме само няколко минути, а софтуерното шифроване може да отнеме няколко часа.

шифроване
Процедура, като например използване на криптографски алгоритъм за превръщане на обикновен текст в шифрован текст, за да се предотврати прочитането на данните от неупълномощени потребители. Съществуват много видове шифроване на данни и те са в основата на защитата на мрежата. Сред най-често срещаните видове са Стандарта за шифроване на данни и шифроване с публичен ключ.

Азбучен указател