HP Client Security

بدء التشغيل

إن المعلومات الواردة في هذا الدليل عرضة للتغيير دون إشعار مسبق. إن الضمانات الخاصة بمنتجات HP وخدماتها هي فقط تلك المعلن عنها بشكل واضح ضمن بنود الضمان الذي يصاحب مثل هذه المنتجات والخدمات. ويجب عدم اعتبار أي مما ورد هنا على أنه بمثابة ضمان إضافي. تخلي شركة HP مسئوليتها عن أي أخطاء فنية أو تحريرية أو أي أخطاء ناتجة عن سهو وردت في هذا المستند.

الإصدار الأول: أغسطس ٢٠١٣

الرقم المرجعي للمستند: 735339-171

جدول المحتويات

١ تقديم حول HP Client Security Manager

يتيح لك برنامج HP Client Security حماية بياناتك وجهازك وهويتك، وبالتالي زيادة حماية الكمبيوتر.

قد تختلف الوحدات النمطية للبرنامج المتاحة لجهاز الكمبيوتر اعتمادًا على طراز جهازك.

قد تكون الوحدات النمطية لبرنامج HP Client Security مثبتَّة مسبقًا أو محملَّة مسبقًا، أو متوفرًة للتنزيل من على موقع HP على الإنترنت. لمزيد من المعلومات، انظر http://www.hp.com.

ملاحظة: تمت كتابة التعليمات الواردة في هذا الدليل على افتراض أنكم قد قمتم بالفعل بتثبيت الوحدات النمطية القابلة للتطبيق لبرنامج HP Client Security.

ميزات HP Client Security

يبين الجدول التالي بالتفصيل الميزات الرئيسية للوحدات النمطية لبرنامج HP Client Security.

الوحدة النمطية	الميزات الرئيسية
HP Client Security Manager	يمكن للمسؤولين تنفيذ الوظائف التالية: • حماية جهاز الكمبيوتر قبل بدء تشغيل Windows • حماية حساب Windows باستخدام المصادقة الفعالة • إدارة عمليات تسجيل الدخول وكلمات المرور لمواقع الويب والتطبيقات • تغيير كلمة المرور الخاصة بنظام التشغيل Windows بسهولة • استخدام بصمات الأصابع لتوفير المزيد من الحماية والراحة • إعداد بطاقة ذكية أو بطاقة غير تلامسية أو بطاقة اقتراب للمصادقة • استخدام هاتف بتقنية Bluetooth كطريقة للتعريف • تعيين رمز PIN لتوسعة خيارات المصادقة • تكوين سياسات تسجيل الدخول والجلسات • النسخ الاحتياطي لبيانات البرنامج واستعادتها • إضافة المزيد من التطبيقات، مثل HP Drive Encryption وHP File Sanitizer وHP Trust Circles وHP Device Access Manager وHP Computrace يمكن للمستخدمين العامين تنفيذ الوظائف التالية: • عرض إعدادات حالة التشفير وDevice Access Manager. • تنشيط Computrace. • تكوين التفضيلات وخيارات النسخ الاحتياطي والاستعادة.

الوحدة النمطية	الميزات الرئيسية
Password Manager	يمكن للمستخدمين العامين تنفيذ الوظائف التالية: • تنظيم وإعداد أسماء المستخدمين وكلمات المرور. • إنشاء كلمات مرور أقوى للحصول على حماية محسنة لحسابات البريد الإلكتروني وحسابات الويب. ويدرج Password Manager ويرسل المعلومات تلقائيًا. • تبسيط عملية تسجيل الدخول مع ميزة تسجيل الدخول الأحادي، التي تتذكر وتطبق تلقائيًا بيانات اعتماد المستخدم. • وضع علامة على الحساب تبين أنه قد تم اكتشافه، وبذلك يتم تنبيهك عن حساب/حسابات أخرى لها بيانات اعتماد مماثلة. • استيراد بيانات تسجيل الدخول من مستعرض معتمد.
HP Drive Encryption (طُرز محددة فقط)	• يوفر تشفيرًا تامًا لكامل حجم محرك القرص الثابت. • يفرض المصادقة قبل التمهيد من أجل فك تشفير البيانات والوصول إليها. • يقدم خيار تنشيط محركات الأقراص ذاتية التشفير (طُرز محددة فقط).
HP Device Access Manager	• يسمح لمديري تكنولوجيا المعلومات بالتحكم بالوصول إلى الأجهزة استنادًا إلى ملفات تعريف المستخدمين. • يمنع المستخدمين غير المصرح لهم من إزالة البيانات باستخدام وسائط التخزين الخارجية، ومن إدخال الفيروسات إلى النظام من الوسائط الخارجية. • يسمح للمسؤولين بتعطيل إمكانية الوصول إلى أجهزة الاتصالات بالنسبة إلى أفراد أو مجموعات مستخدمين محددة.
HP Trust Circles	• يوفر الحماية للملفات والمستندات. • يشفر هذا التطبيق الملفات الموجودة في مجلدات خاصة يحددها المستخدم، بما يوفر لها الحماية داخل دائرة ثقة. • يسمح باستخدام الملفات ومشاركتها فقط من قبل أفراد دائرة الثقة.
Theft Recovery (Computrace، يتم شراؤه على حدة)	• يتطلب الشراء المنفصل لاشتراكات التتبع والتعقب للتنشيط. • يوفر تتبع أصول آمن. • يرصد نشاط المستخدم، فضلاً عن تغييرات الأجهزة والبرامج. • يظل نشطًا حتى إذا تمت إعادة تنسيق محرك القرص الثابت أو استبداله.

وصف منتج HP Client Security وأمثلة على استخداماته العامة

تشتمل معظم منتجات HP Client Security على كلٍ من مصادقة المستخدم (عادةً من خلال كلمة مرور)، ونسخة احتياطية خاصة بالمسؤول للتمكن من الوصول إذا تم فقد كلمات المرور، أو كانت غير متوفرة، أو تم نسيانها، أو في أي وقت تحتاج حماية الشركات الوصول.

ملاحظة: وقد تم تصميم بعض منتجات HP Client Security لتقييد إمكانية الوصول إلى البيانات. ويجب أن تكون البيانات مشفرةً عندما تكون مهمة جدًا ويفضل المستخدم أن يفقد المعلومات على أن يتركها تنكشف. ويوصى بنسخ جميع البيانات احتياطيًا في مكان آمن.

Password Manager

يخزن Password Manager أسماء المستخدمين وكلمات المرور، ويمكن استخدامه بهدف:

- حفظ أسماء تسجيل الدخول وكلمات المرور للوصول إلى الإنترنت أو البريد الإلكتروني.
- تسجيل دخول المستخدم تلقائيًا إلى موقع ويب أو إلى بريد إلكتروني.
- إدارة وتنظيم المصادقة.
- تحديد أصول موقع ويب أو شبكة والوصول إلى الارتباط مباشرةً.

- عرض أسماء وكلمات المرور عند الضرورة.
- وضع علامة على الحساب تبين أنه قد تم اكتشافه، وبذلك يتم تنبيهك عن حساب/حسابات أخرى لها بيانات اعتماد مماثلة.
- استيراد بيانات تسجيل الدخول من مستعرض معتمد.

المثال الأول: تقوم وكيلة شراء لدى شركة تصنيع كبيرة بتنفيذ معظم تعاملاتها عبر الإنترنت. كما أنها في كثير من الأحيان تزور العديد من مواقع الويب الشهيرة التي تتطلب معلومات تسجيل الدخول. وهي تدرك تمامًا مسائل الحماية فلا تستخدم كلمة المرور نفسها على كل حساب. قررت وكيلة الشراء استخدام Password Manager ليلائم بين ارتباطات الويب وأسماء المستخدمين وكلمات المرور المختلفة. وعندما تنتقل إلى موقع ويب لتسجيل الدخول، يقدم Password Manager بيانات الاعتماد تلقائيًا. وإذا أردت عرض أسماء المستخدمين وكلمات المرور، يمكن تكوين Password Manager بحيث يتم عرضها.

ويمكن أيضًا استخدام Password Manager لإدارة وتنظيم عمليات المصادقة. وتسمح هذه الأداة للمستخدم بتحديد أصول صفحة الويب أو الشبكة والوصول إلى الارتباط مباشرةً. ويمكن للمستخدم أيضًا عرض أسماء المستخدمين وكلمات المرور عند الضرورة.

المثال الثاني: تمت ترقية موظف يعمل بجد وسيقوم الآن بإدارة قسم المحاسبة بأكمله. يجب على الفريق تسجيل الدخول إلى عدد كبير من حسابات العملاء على الويب، كل منها يستخدم معلومات تسجيل دخول مختلفة. ويجب مشاركة معلومات تسجيل الدخول هذه مع بقية العمال، لذلك فالسرية مسألة أساسية. يقرر الموظف تنظيم جميع ارتباطات الويب، وأسماء مستخدمي الشركة، وكلمات المرور ضمن Password Manager. وفور اكتمال هذا العمل، ينشر الموظف Password Manager للموظفين حتى يتمكنوا من العمل على حسابات الويب دون أن يعرفوا أبدًا بيانات اعتماد تسجيل الدخول التي يستخدمونها.

HP Drive Encryption (طُرز محددة فقط)

يتم استخدام HP Drive Encryption لتقييد الوصول إلى البيانات على كامل محرك القرص الثابت لجهاز كمبيوتر أو على محرك أقراص ثانوي. يمكن لتطبيق Drive Encryption أيضًا إدارة محركات الأقراص ذاتية التشفير.

المثال الأول: يريد طبيب التأكد من أنه هو وحده يمكنه الوصول إلى أية بيانات على محرك القرص الثابت بجهاز الكمبيوتر الخاص به. يُنشِّط الطبيب Drive Encryption، الذي يطلب المصادقة قبل التمهيد قبل تسجيل الدخول إلى Windows. بعد الإعداد، لا يمكن الوصول إلى محرك القرص الثابت دون كلمة مرور قبل بدء تشغيل نظام التشغيل. يمكن للطبيب مواصلة تحسين حماية محركات الأقراص عن طريق اختيار تشفير البيانات من خلال خيار التشفير الذاتي لمحرك الأقراص.

المثال الثاني: يريد مسؤول مستشفى أن يضمن أن الأطباء والموظفين المصرح لهم وحدهم يمكنهم الوصول إلى أية بيانات على أجهزة الكمبيوتر المحلية الخاصة بهم دون مشاركة كلمات مرورهم الشخصية. يضيف قسم تكنولوجيا المعلومات المسؤول والأطباء وجميع الموظفين المصرح لهم كمستخدمين لتطبيق Drive Encryption. والآن يمكن لأفراد طاقم العاملين المصرح لهم فقط تمهيد الكمبيوتر أو المجال باستخدام أسماء المستخدمين وكلمات المرور الخاصة بهم.

HP Device Access Manager (طُرز محددة فقط)

يسمح HP Device Access Manager للمسؤول بتقييد إمكانية الوصول إلى الأجهزة وإدارتها. يمكن استخدام Device Access Manager لمنع الوصول غير المصرح به إلى محرك القرص المحمول من نوعية USBعندما يمكن نسخ البيانات. كما يمكنه تقييد الوصول إلى محركات الأقراص المضغوطة/ أقراص DVD، والسيطرة على محركات الأقراص المحمولة من نوعية USB، واتصال الشبكة، وهكذا. ومثال على ذلك، هو أن يحتاج الموردون الخارجيون الوصول إلى أجهزة الكمبيوتر الخاصة بشركة، ولكن لا ينبغي أن يكونوا قادرين على نسخ البيانات إلى محركات الأقراص المحمولة من نوعية USB.

المثال الأول: غالبًا ما يتعامل مدير شركة التوريد الطبي مع السجلات الطبية الشخصية جنبًا إلى جنب مع معلومات شركته. ويحتاج الموظفون إلى الوصول إلى هذه البيانات، ولكن المهم للغاية ألا تتم إزالة البيانات من جهاز الكمبيوتر عن طريق محرك أقراص محمول من نوعية USB أو أية وسائط تخزين خارجية أخرى. الشبكة آمنة، ولكن أجهزة الكمبيوتر تتضمن ناسخات أقراص مضغوطة ومنافذ USB يمكن أن تسمح للبيانات أن يتم نسخها أو سرقتها. يستخدم المدير Device Access Manager لتعطيل منافذ USB وناسخات الأقراص المضغوطة بحيث لا يمكن استخدامها. وعلى الرغم من حظر منافذ USB، يستمر الماوس ولوحات المفاتيح في العمل.

المثال الثاني: شركة تأمين لا تريد أن يقوم موظفوها بتثبيت أو تحميل البرامج أو البيانات الشخصية من المنزل. وبعض الموظفين يحتاجون إلى الوصول إلى منفذ USB على جميع أجهزة الكمبيوتر. يستخدم مدير تكنولوجيا المعلومات Device Access Manager لتمكين الوصول بالنسبة إلى بعض الموظفين مع حظر إمكانية الوصول الخارجي للآخرين.

Computrace (يتم شراؤه على حدة)

يُعد Computrace (يتم شراؤه على حدة) خدمة يمكنها تتبع مكان وجود جهاز كمبيوتر مسروق عندما يصل المستخدم إلى الإنترنت. ويمكن لتطبيق Computrace المساعدة أيضًا في الإدارة عن بُعد وعلى تحديد موقع أجهزة الكمبيوتر، فضلاً عن مراقبة استخدام الكمبيوتر وتطبيقاته.

المثال الأول: أوعز مدير مدرسة إلى قسم تكنولوجيا المعلومات بتتبع جميع أجهزة الكمبيوتر في مدرسته. بعد إجراء جرد لأجهزة الكمبيوتر، سجل مسؤول تكنولوجيا المعلومات جميع أجهزة الكمبيوتر على Computrace بحيث يمكن تتبعها في حال سرقتها. في الآونة الأخيرة، أدركت المدرسة أن العديد من أجهزة الكمبيوتر قد فُقدت، لذلك نبه مسؤول تكنولوجيا المعلومات السلطات ومسؤولي Computrace. وتم تحديد موقع أجهزة الكمبيوتر وأعادتها السلطات إلى المدرسة.

المثال الثاني: تحتاج شركة عقارات لإدارة أجهزة كمبيوتر في جميع أنحاء العالم وتحديثها. وهم يستخدمون Computrace لمراقبة أجهزة الكمبيوتر وتحديثها دون الحاجة إلى إرسال شخص مختص في تكنولوجيا المعلومات إلى مكان كل كمبيوتر.

تحقيق أهداف الحماية الرئيسية

يمكن للوحدات النمطية لتطبيق HP Client Security العمل معًا لتوفير حلول لمجموعة متنوعة من مشكلات الحماية، بما في ذلك أهداف الحماية الرئيسية التالية:

- الحماية ضد السرقة المستهدفة
- تقييد الوصول إلى البيانات الحساسة
- منع الوصول غير المصرح به من مواقع داخلية أو خارجية
- وضع سياسات كلمات مرور قوية

الحماية ضد السرقة المستهدفة

ومثال على السرقة المستهدفة هو سرقة جهاز كمبيوتر يحتوي على بيانات سرية ومعلومات عملاء في نقطة تفتيش حماية في المطار. تساعد الميزات التالية في الحماية من السرقة المستهدفة:

- تساعد ميزة المصادقة قبل التمهيد، في حال تمكينها، في منع الوصول إلى نظام التشغيل.
  - HP Client Security — انظر HP Client Security في صفحة ١١.
  - HP Drive Encryption — انظر HP Drive Encryption (طُرز محددة فقط) في صفحة ٢٦.
- يساعد التشفير على ضمان أن البيانات لا يمكن الوصول إليها حتى لو تمت إزالة محرك القرص الثابت وتركيبه على نظام غير محمي.
- ويستطيع Computrace تتبع موقع الكمبيوتر بعد السرقة.
  - Computrace — انظر Theft recovery (طُرز محددة فقط) في صفحة ٤٨.

تقييد الوصول إلى البيانات الحساسة

لنفترض أن مراجع عقود يعمل في الموقع وقد أعطيت له إمكانية الوصول إلى الكمبيوتر لمراجعة البيانات المالية الحساسة. وأنت لا تريد أن يكون المراجع قادرًا على طباعة الملفات أو حفظها على جهاز قابل للكتابة، مثل القرص المضغوط. تساعد الميزة التالية على تقييد الوصول إلى البيانات:

- يتيح HP Device Access Manager لمديري تكنولوجيا المعلومات تقييد الوصول إلى أجهزة الاتصالات بحيث لا يمكن نسخ المعلومات الحساسة من محرك القرص الثابت. انظر طريقة عرض النظام في صفحة ٣٩.

منع الوصول غير المصرح به من مواقع داخلية أو خارجية

يمثل الوصول غير المصرح به إلى جهاز كمبيوتر تجاري غير محمي خطرًا حقيقيًا للغاية على موارد شبكة الشركة، مثل المعلومات الواردة من قسم الخدمات المالية أو المسؤولين التنفيذيين أو فريق البحث والتطوير، وعلى المعلومات الخاصة مثل سجلات المرضى أو السجلات المالية الشخصية. وتساعد الميزات التالية على منع الوصول غير المصرح به:

- تساعد ميزة المصادقة قبل التمهيد، في حال تمكينها، في منع الوصول إلى نظام التشغيل. (انظر HP Drive Encryption (طُرز محددة فقط) في صفحة ٢٦.
- يساعد HP Client Security على ضمان أن المستخدمين غير المصرح لهم لا يمكنهم الحصول على كلمات المرور أو الوصول إلى التطبيقات المحمية بكلمة مرور. انظر HP Client Security في صفحة ١١.
- يتيح HP Device Access Manager لمديري تكنولوجيا المعلومات تقييد الوصول إلى الأجهزة القابلة للكتابة بحيث لا يمكن نسخ المعلومات الحساسة من محرك القرص الثابت. انظر HP Device Access Manager (طُرز محددة فقط) في صفحة ٣٨.

وضع سياسات كلمات مرور قوية

اذا أقرت شركة سياسة تتطلب استخدام نهج كلمات مرور قوية لعشرات من التطبيقات المستندة إلى الويب وقواعد البيانات، يوفر Password Manager مخزنًا محميًا لكلمات المرور ويقدم راحة من خلال ميزة تسجيل الدخول الأحادي. انظر Password Manager في صفحة ١٦.

عناصر الحماية الإضافية

تعيين أدوار الحماية

في إدارة حماية الكمبيوتر (ولا سيما في المؤسسات الكبيرة)، إحدى الممارسات المهمة هي تقسيم المسؤوليات والحقوق بين أنواع مختلفة من المسؤولين والمستخدمين.

ملاحظة: وفي المؤسسات الصغيرة أو في حالة الاستخدام الفردي، قد يقوم الشخص نفسه بكل هذه الأدوار.

في HP Client Security، يمكن تقسيم واجبات الحماية والامتيازات ضمن الأدوار التالية:

- موظف الحماية — يحدد مستوى الحماية للشركة أو الشبكة ويحدد ميزات الحماية التي يتم نشرها مثل Drive Encryption.

ملاحظة: يمكن تخصيص العديد من ميزات HP Client Security من قِبل موظف الحماية بالتعاون مع HP. لمزيد من المعلومات، انظر http://www.hp.com.

- مسؤول تكنولوجيا المعلومات — يطبق ميزات الحماية التي يحددها موظف الحماية ويديرها. ويمكنه أيضًا تمكين بعض الميزات وتعطيلها. على سبيل المثال، إذا كان موظف الحماية قد قرر نشر البطاقات الذكية، يمكن لمسؤول تكنولوجيا المعلومات أن يمكّن وضع كل من كلمة المرور والبطاقة الذكية.
- المستخدم — يستخدم ميزات الحماية. على سبيل المثال، إذا كان موظف الحماية ومسؤول تكنولوجيا المعلومات قد مكّنا البطاقات الذكية للنظام، يمكن للمستخدم تعيين رمز PIN للبطاقة الذكية واستخدام البطاقة للمصادقة.

تنبيه: ونحث المسؤولين على اتباع "أفضل الممارسات" في تقييد امتيازات المستخدم النهائي وتقييد وصول المستخدم.

لا ينبغي منح المستخدمين غير المصرح لهم امتيازات المسؤول.

إدارة كلمات مرور HP Client Security

تتم حماية معظم ميزات HP Client Security بواسطة كلمات المرور. يسرد الجدول التالي كلمات المرور الشائعة، والوحدة النمطية للبرنامج حيث يتم تعيين كلمة المرور ووظيفة كلمة المرور.

كما يتم كذلك توضيح كلمات المرور التي يتم تعيينها واستخدامها من قِبل مسؤولي تكنولوجيا المعلومات وحدهم. ويمكن تعيين جميع كلمات المرور الأخرى من قِبل المستخدمين أو المسؤولين العاديين.

كلمة مرور HP Client Security	يتم تعيينها في الوحدة النمطية التالية	الوظيفة
كلمة مرور تسجيل الدخول إلى Windows	لوحة تحكم Windows أو HP Client Security	يمكن استخدامها لتسجيل الدخول اليدوي وللمصادقة للوصول إلى ميزات HP Client Security المختلفة.
كلمة مرور النسخ الاحتياطي والاستعادة لبرنامج HP Client Security	HP Client Security، عن طريق المستخدم الفرد	يحمي الوصول إلى ملف النسخ الاحتياطي والاستعادة لبرنامج HP Client Security.
رمز PIN للبطاقة الذكية	Credential Manager (إدارة بيانات الاعتماد)	يمكن استخدامها كمصادقة متعددة العوامل. يمكن استخدامها كمصادقة Windows. تصادق على مستخدمي Drive Encryption، في حالة تحديد البطاقة الذكية.

إنشاء كلمة مرور آمنة

عند إنشاء كلمات المرور، يجب عليك أولاً اتباع أية مواصفات تم تعيينها من قِبل البرنامج. على الرغم من ذلك، وبشكل عام، يمكنك التفكير في التوجيهات التالية لمساعدتك في إنشاء كلمات مرور قوية تقلل من فرص انكشاف كلمة مرورك:

- استخدم كلمات مرور تتكون من أكثر من ٦ أحرف، ويفضل أكثر من ٨.
- نوّع من حالة الأحرف في جميع أنحاء كلمة المرور.
- كلما أمكن، امزج بين الرموز الأبجدية الرقمية، وضمِّن الرموز الخاصة وعلامات الترقيم.
- استبدل الأحرف بالرموز الخاصة أو الأرقام في الكلمة الأساسية. على سبيل المثال، يمكنك استخدام الرقم ١ بدلاً من الحرف I أو L.
- اجمع بين كلمات من لغتين أو أكثر.
- قسّم الكلمة أو العبارة بأرقام أو رموز خاصة في الوسط، على سبيل المثال، "Mary2-2Cat45".
- لا تستخدم كلمة المرور التي يمكن أن تظهر في القاموس.
- لا تستخدم اسمك ككلمة مرور ولا أية معلومات شخصية أخرى، مثل تاريخ ميلادك أو أسماء الحيوانات الأليفة، أو اسم الأم قبل الزواج، حتى لو قمت بهجائها بالمقلوب.
- غيِّر كلمات المرور بشكل منتظم. يمكنك التغيير من خلال زيادة بضعة رموز فقط.
- إذا كتبت كلمة مرورك، فلا تخبئها في مكان ظاهر عادةً وقريب جدًا من جهاز الكمبيوتر.
- لا تحفظ كلمة المرور في ملف، مثل ملف بريد إلكتروني، على جهاز الكمبيوتر.
- لا تعلم الآخرين بالحسابات أو تخبر أحدًا بكلمة مرورك.

النسخ الاحتياطي لبيانات الاعتماد والإعدادات

يمكنك استخدام أداة النسخ الاحتياطي والاستعادة الموجودة ضمن HP Client Security كموقع مركزي يمكنك من خلاله إجراء النسخ الاحتياطي والاستعادة لبيانات اعتماد الحماية من بعض الوحدات النمطية المثبتة لبرنامج HP Client Security.

٢ بدء التشغيل

لتكوين HP Client Security للاستخدام مع بيانات اعتمادك، ابدأ تشغيل HP Client Security بإحدى الطرق التالية. بمجرد إكمال مستخدم للمعالج، لا يمكن لذلك المستخدم بدء تشغيله مرة أخرى.

١. من شاشة Start (ابدأ) أو Apps (التطبيقات)، انقر فوق أو اضغط على تطبيق **HP Client Security** (في نظام التشغيل Windows 8).

– أو –

من سطح مكتب Windows، انقر فوق أو اضغط على **الأداة الذكية لبرنامج HP Client Security** (في نظام التشغيل Windows 7).

– أو –

من سطح مكتب Windows، انقر نقرًا مزدوجًا فوق أيقونة **HP Client Security** في منطقة الإعلام بأقصى يمين شريط المهام، أو اضغط عليها ضغطًا مزدوجًا.

– أو –

من سطح مكتب Windows، انقر فوق أو اضغط على أيقونة **HP Client Security** في منطقة الإعلام، ثم حدد **Open HP Client Security** (فتح HP Client Security).

٢. يتم بدء تشغيل معالج إعداد برنامج HP Client Security مع عرض صفحة الترحيب.

٣. اقرأ شاشة الترحيب، وأكد هويتك من خلال كتابة كلمة مرور Windows، ثم انقر فوق أو اضغط على **Next** (التالي).

إذا لم تنشئ بعد كلمة مرور Windows، فستتم مطالبتك بإنشاء كلمة مرور. ويلزم توفير كلمة مرور Windows لحماية حساب Windows من وصول الأشخاص غير المخولين ولاستخدام ميزات HP Client Security.

٤. في صفحة HP SpareKey، حدد ثلاثة أسئلة للحماية. أدخل إجابة عن كل سؤال، ثم انقر فوق **Next** (التالي). كما أن الأسئلة المخصصة متاحة أيضًا. للحصول على مزيد من المعلومات، انظر HP SpareKey — استرداد كلمة المرور في صفحة ١٢.

٥. في صفحة بصمات الأصابع، سجل الحد الأدنى لعدد بصمات الأصابع المطلوبة على الأقل، ثم انقر فوق أو اضغط على **Next** (التالي). للحصول على مزيد من المعلومات، انظر بصمات الأصابع في صفحة ١١.

٦. في صفحة Drive Encryption، نشِّط ميزة التشفير، وانسخ مفتاح التشفير احتياطيًا، ثم انقر فوق أو اضغط على **Next** (التالي). للحصول على مزيد من المعلومات، انظر تعليمات برنامج HP Drive Encryption.

ملاحظة: ينطبق ذلك على السيناريو حيث يكون المستخدم مسؤولاً، ولم يتم تكوين معالج إعداد HP Client Security من قِبل مسؤول سابقًا.

٧. في الصفحة الأخيرة من المعالج، انقر فوق أو اضغط على **Finish** (إنهاء).

توفر هذه الصفحة حالة الميزات وبيانات الاعتماد.

٨. يضمن معالج إعداد HP Client Security تنشيط ميزات المصادقة في الوقت المناسب وFile Sanitizer. للحصول على مزيد من المعلومات، راجع تعليمات برنامج HP Device Access Manager وتعليمات برنامج HP File Sanitizer.

ملاحظة: ينطبق ذلك على السيناريو حيث يكون المستخدم مسؤولاً، ولم يتم تكوين معالج إعداد HP Client Security من قِبل مسؤول سابقًا.

فتح HP Client Security

يمكنك فتح تطبيق HP Client Security بإحدى الطرق التالية:

ملاحظة: يجب إكمال معالج إعداد HP Client Security قبل التمكن من بدء تشغيل تطبيق HP Client Security.

- من شاشة Start (ابدأ) أو Apps (التطبيقات)، انقر فوق أو اضغط على تطبيق **HP Client Security**.

– أو –

من سطح مكتب Windows، انقر فوق أو اضغط على الأداة الذكية **HP Client Security** (في نظام التشغيل Windows 7).

– أو –

من سطح مكتب Windows، انقر نقرًا مزدوجًا فوق أيقونة **HP Client Security** في منطقة الإعلام بأقصى يمين شريط المهام، أو اضغط عليها ضغطًا مزدوجًا.

– أو –

من سطح مكتب Windows، انقر فوق أو اضغط على أيقونة **HP Client Security** في منطقة الإعلام، ثم حدد **Open HP Client Security** (فتح HP Client Security).

٣ دليل الإعداد السهل للشركات الصغيرة

تم تصميم هذا الفصل لشرح الخطوات الأساسية لتفعيل الخيارات الأكثر شيوعًا وفائدةً في HP Client Security for Small Business. تتيح لك العديد من الأدوات والخيارات في هذا البرنامج الضبط الدقيق لتفضيلاتك وتعيين ميزة التحكم في الوصول. ويركز دليل الإعداد السهل على تشغيل كل وحدة نمطية للبرنامج بأقل قدر من الجهد والوقت في الإعداد. للحصول على معلومات إضافية، حدد الوحدة النمطية التي تهمك، ثم انقر فوق **?** أو زر Help (تعليمات) في الزاوية العلوية اليمنى. وسيعرض هذا الزر المعلومات تلقائيًا لمساعدتك فيما يخص النافذة المعروضة على الشاشة حاليًا.

بدء التشغيل

١. من سطح مكتب Windows، افتح HP Client Security بالنقر نقرًا مزدوجًا فوق أيقونة **HP Client Security** في منطقة الإعلام بأقصى يمين شريط المهام.

٢. أدخل كلمة مرور Windows الخاصة بك، أو أنشئ كلمة مرور Windows.

٣. أكمل إعداد HP Client Security.

حتى لا يطلب منك HP Client Security بيانات المصادقة سوى مرة واحدة خلال تسجيل الدخول إلى Windows، انظر ميزات الحماية في صفحة ٢٤.

Password Manager

كل شخص لديه عدد كبير من كلمات المرور - خصوصا إذا كان يصل إلى مواقع الويب بشكل منتظم أو يستخدم التطبيقات التي تتطلب تسجيل الدخول. والمستخدم العادي إما أنه يستخدم كلمة المرور نفسها لجميع التطبيقات والمواقع، أو أنه يسعى ليكون مبدعًا وينسى سريعًا أية كلمة مرور تخص أي تطبيق.

ويمكن لتطبيق Password Manager أن يتذكر تلقائيًا كلمات مرورك أو يعطيك القدرة على تمييز المواقع التي تريد تذكرها وتلك التي تريد حذفها. بمجرد تسجيل الدخول إلى جهاز الكمبيوتر، يوفر Password Manager كلمات المرور وبيانات المصادقة الخاصة بك للتطبيقات أو مواقع الويب المشتركة.

وعند الوصول إلى أي تطبيق أو موقع ويب يتطلب بيانات اعتماد، يتعرف Password Manager تلقائيًا على الموقع، ويسأل إذا كنت تريد من البرنامج أن يتذكر معلوماتك. إذا كنت تريد استبعاد بعض المواقع، يمكنك رفض الطلب.

لتبدأ في حفظ مواقع الويب، وأسماء المستخدمين وكلمات المرور:

١. على سبيل المثال، انتقل إلى موقع ويب أو تطبيق مشارك، ثم انقر فوق أيقونة Password Manager في الزاوية العلوية اليسرى من صفحة الويب لإضافة مصادقة صفحة الويب.

٢. أطلق اسمًا على الارتباط (اختياري)، وأدخل اسم المستخدم وكلمة المرور في Password Manager.

٣. عند الانتهاء، انقر فوق زر **OK** (موافق).

٤. يمكن لتطبيق Password Manager أيضًا أن يحفظ اسم المستخدم وكلمات المرور الخاصة بمشاركات الشبكة أو محركات أقراص الشبكة المعينة.

عرض وإدارة بيانات المصادقة المحفوظة في Password Manager

يسمح لك Password Manager بعرض بيانات المصادقة الخاصة بك وإدارتها ونسخها احتياطيًا وتشغيلها من موقع مركزي. كما يتيح Password Manager تشغيل المواقع المحفوظة من نظام التشغيل Windows.

لفتح Password Manager، استخدام مجموعة المفاتيح Ctrl+ مفتاح Windows+h لفتحPassword Manager، ثم انقر فوق **Log in** (تسجيل الدخول) لتشغيل الاختصار المحفوظ ومصادقته.

يسمح خيار **Edit** (تعديل) في Password Manager بعرض وتعديل الاسم واسم تسجيل الدخول، وحتى الكشف عن كلمات المرور.

يسمح HP Client Security for Small Business بالنسخ الاحتياطي لجميع بيانات الاعتماد والإعدادات و/أو نسخها على كمبيوتر آخر.

HP Device Access Manager

يمكن استخدام Device Access Manager لتقييد استخدام مختلف أجهزة التخزين الداخلية والخارجية بحيث تبقى بياناتك على محرك القرص الثابت محمية ولا تغادر حدود عملك. على سبيل المثال، يمكنك السماح لمستخدم بالوصول إلى بياناتك ومنعه من نسخها على قرص مضغوط، أو مشغل الموسيقى الشخصية، أو جهاز ذاكرة USB.

١. افتح **Device Access Manager** (انظر فتح Device Access Manager في صفحة ٣٨).

يتم عرض عملية الوصول للمستخدم الحالي.

٢. لتغيير إمكانية الوصول للمستخدمين أو المجموعات أو الأجهزة، انقر أو اضغط على **Change** (تغيير). للحصول على مزيد من المعلومات، انظر طريقة عرض النظام في صفحة ٣٩.

HP Drive Encryption

يتم استخدام HP Drive Encryption لحماية بياناتك عن طريق تشفير محرك القرص الثابت بأكمله. وستبقى البيانات على محرك القرص الثابت محمية حتى لو سُرق جهاز الكمبيوتر الخاص بك و/أو إذا تمت إزالة محرك القرص الثابت من الكمبيوتر الأصلي ووضعه في كمبيوتر آخر.

وهناك فائدة حماية إضافية تتمثل في أن Drive Encryption يطلب منك المصادقة بشكل صحيح باستخدام اسم المستخدم وكلمة المرور قبل بدء نظام التشغيل. وتدعى هذه العملية المصادقة قبل التمهيد.

ولتسهيل الأمر عليك، تقوم وحدات نمطية برمجية متعددة بمزامنة كلمات المرور تلقائيًا، بما في ذلك حسابات مستخدمي Windows ومجالات المصادقة وHP Drive Encryption وPassword Manager وHP Client Security.

لإعداد HP Drive Encryption أثناء الإعداد الأولي عن طريق معالج إعداد HP Client Security، انظر بدء التشغيل في صفحة ٧.

٤ HP Client Security

تعد صفحة HP Client Security الرئيسية الموقع المركزي للوصول السهل إلى ميزات HP Client Security وتطبيقاته وإعداداته. وتنقسم الصفحة الرئيسية إلى ثلاثة أقسام:

- **DATA** (البيانات) — لتوفير إمكانية الوصول إلى التطبيقات المستخدمة لإدارة حماية البيانات.
- **DEVICE** (الجهاز) — لتوفير إمكانية الوصول إلى التطبيقات المستخدمة لإدارة حماية الأجهزة.
- **IDENTITY** (الهوية) — لتوفير إمكانية التسجيل وإدارة بيانات اعتماد المصادقة.

حرك المؤشر فوق لوحة التطبيق لعرض وصف التطبيق.

يمكن أن يتيح تطبيق HP Client Security روابط لإعدادات المستخدم وإعدادات المسؤول أسفل الصفحة. يوفر HP Client Security وصولاً إلى الإعدادات والميزات المتقدمة بالضغط على أو النقر فوق أيقونة **Gear** (الترس) (الإعدادات).

ميزات الهوية وتطبيقاتها وإعداداتها

تساعدك ميزات الهوية وتطبيقاتها وإعداداتها المتاحة من خلال HP Client Security على إدارة جوانب متعددة من الهوية الرقمية. انقر فوق أو اضغط على إحدى اللوحات التالية بصفحة HP Client Security الرئيسية، ثم أدخل كلمة مرور Windows:

- **Fingerprints** (بصمات الأصابع) — لتسجيل بيانات اعتماد بصمات الأصابع الخاصة بك وإدارتها.
- **SpareKey** — لإعداد وإدارة بيانات اعتماد HP SpareKey التي يمكن استخدامها لتسجيل الدخول إلى جهازك في حالة فقدان بيانات اعتمادك الأخرى أو وضعها في غير موضعها. ويتيح أيضًا إعادة تعيين كلمة مرورك التي نسيتها.
- **Windows Password** (كلمة مرور Windows) — لإتاحة الوصول السهل لتغيير كلمة مرور Windows.
- **Bluetooth Devices**(أجهزة Bluetooth) — لإتاحة تسجيل أجهزة Bluetooth وإدارتها.
- **Cards**(البطاقات) — لإتاحة تسجيل البطاقات الذكية والبطاقات غير التلامسية وبطاقات الاقتراب وإدارتها.
- **PIN** (رمز PIN) — لإتاحة تسجيل بيانات اعتماد رمز PIN وإدارتها.
- **RSA SecurID** — لإتاحة تسجيل بيانات اعتماد RSA SecurID وإدارتها (إذا توفر الإعداد المطلوب).
- **Password Manager** — لإتاحة إدارة كلمات المرور للحسابات والتطبيقات الخاصة بك على الإنترنت.

بصمات الأصابع

يرشدك معالج إعداد HP Client Security خلال عملية إعداد أو "تسجيل" بصمات الأصابع.

ويمكنك أيضًا تسجيل أو حذف بصمات الأصابع بصفحة بصمات الأصابع التي يمكنك دخولها بالنقر فوق أو الضغط على أيقونة **Fingerprints** (بصمات الأصابع) بصفحة HP Client Security الرئيسية.

١. في صفحة بصمات الأصابع، يمكنك التمرير بأحد أصابعك حتى يتم تسجيله بنجاح.

وعدد الأصابع اللازم للتسجيل موضح في هذه الصفحة. ويُفضل السّبابة أو الإصبع الأوسط.

٢. لحذف بصمات الأصابع المسجلة مسبقًا، انقر فوق أو اضغط على **Delete** (حذف).

٣. لتسجيل أصابع إضافية، انقر فوق أو اضغط على **Enroll an additional fingerprint** (تسجيل بصمة إصبع إضافية).

٤. انقر فوق أو اضغط على **Save** (حفظ) قبل الانتقال من الصفحة.

⚠ **تنبيه:** في حالة تسجيل بصمات الأصابع من خلال المعالج، لا يتم حفظ معلومات بصمات الأصابع حتى تنقر فوق **Next** (التالي). وإذا تركت الكمبيوتر دون استخدام لبرهة، أو أغلقت البرنامج، **فلن** يتم حفظ التغييرات التي أجريتها.

- للوصول إلى إعدادات المسؤول لبصمات الأصابع، حيث يمكن أن يحدد المسؤولون إعدادات التسجيل والدقة وغيرها من الإعدادات، انقر فوق أو اضغط على **Administrative Settings** (إعدادات المسؤول) (يلزم توفر امتيازات المسؤول).
- للوصول إلى إعدادات المستخدم الخاصة ببصمات الأصابع، حيث يمكنك أن تحدد الإعدادات التي تتحكم في شكل وطريقة تمييز بصمة الإصبع، انقر فوق أو اضغط على **User Settings** (إعدادات المستخدم).

إعدادات المسؤول لبصمات الأصابع

يمكن أن يحدد المسؤولون إعدادات التسجيل والدقة وغيرها من الإعدادات لقارئ بصمة الإصبع. ويلزم توفر امتيازات المسؤول.

- للوصول إلى إعدادات المسؤول لبيانات اعتماد بصمة الإصبع، انقر فوق أو اضغط على **Administrative Settings** (إعدادات المسؤول) في صفحة بصمات الأصابع.
  - **User enrollment** (تسجيل المستخدم) — اختر أقل وأقصى عدد لبصمات الأصابع المسموح للمستخدم بتسجيلها.
  - **Recognition** (التمييز) — حرك شريط التمرير لضبط الحساسية المستخدمة بواسطة قارئ بصمة الإصبع عندما تمرر إصبعك.

    في حالة عدم تمييز بصمة الإصبع بصورة مستمرة، فقد تحتاج إلى تحديد إعداد تمييز أدنى. ويزيد الإعداد الأعلى الحساسية تجاه التنوعات في تمريرات بصمة الإصبع وبالتالي يقلل من احتمال القبول الخاطئ. ويوفر الإعداد **Medium-High** (متوسط - عالٍ) مزيجًا جيدًا من الحماية والراحة.

إعدادات المستخدم الخاصة ببصمات الأصابع

في صفحة إعدادات المستخدم الخاصة ببصمات الأصابع، يمكنك أن تحدد الإعدادات التي تتحكم في شكل وطريقة تمييز بصمة الإصبع.

- للوصول إلى إعدادات المستخدم لبيانات اعتماد بصمة الإصبع، انقر فوق أو اضغط على **User Settings** (إعدادات المستخدم) في صفحة بصمات الأصابع.
  - **Enable sound feedback** (تمكين التعليقات الصوتية) — بشكل افتراضي، يتيح HP Client Security ميزة التعليقات الصوتية عند تمرير بصمة الإصبع، حيث يتم تشغيل أصوات مختلفة لأحداث برامج معينة. ويمكنك تعيين أصوات جديدة لهذه الأحداث من خلال علامة التبويب "Sounds" (أصوات) في إعداد الصوت في لوحة تحكم Windows، أو لتعطيل التعليقات الصوتية، ألغِ تحديد خانة الاختيار.
  - **Show scan quality feedback** (عرض تعليقات حول جودة المسح) — لعرض جميع التمريرات، بغض النظر عن الجودة، حدد خانة الاختيار. ولعرض التمريرات ذات الجودة الجيدة فقط، ألغِ تحديد خانة الاختيار.

HP SpareKey — استرداد كلمة المرور

يتيح لك تطبيق HP SpareKey التمكن من الوصول إلى الكمبيوتر (في الأنظمة الأساسية المدعومة) من خلال الإجابة عن أسئلة الحماية الثلاثة.

يطالبك HP Client Security بإعداد HP SpareKey الشخصي الخاص بك أثناء الإعداد الأولي في معالج إعداد HP Client Security.

لإعداد HP SpareKey الخاص بك:

١. في صفحة HP SpareKey في المعالج، حدد ثلاثة أسئلة للحماية، ثم أدخل إجابة عن كل سؤال.

   يمكنك تحديد سؤال من قائمة محددة مسبقًا أو كتابة سؤالك الخاص.

٢. انقر فوق أو اضغط على **Enroll** (تسجيل).

لحذف HP SpareKey الخاص بك:

- انقر فوق أو اضغط على **Delete your SpareKey** (حذف HP SpareKey الخاص بك).

بعد إعداد SpareKey الخاص بك، يمكنك الوصول إلى الكمبيوتر باستخدام SpareKey الخاص بك من شاشة تسجيل دخول المصادقة عند بدء التشغيل أو شاشة ترحيب Windows.

يمكنك تحديد أسئلة مختلفة أو تغيير إجاباتك في صفحة SpareKey، والتي يمكن الوصول إليها من لوحة استرداد كلمة المرور في صفحة HP Client Security الرئيسية.

للوصول إلى إعدادات HP SpareKey، حيث يمكن أن يحدد المسؤول الإعدادات المتعلقة ببيانات اعتماد HP SpareKey، انقر فوق **Settings** (الإعدادات) (يلزم توفر امتيازات المسؤول).

إعدادات HP SpareKey

في صفحة إعدادات HP SpareKey، يمكنك أن تحدد الإعدادات التي تتحكم في طريقة واستخدام بيانات اعتماد HP SpareKey.

▲ لبدء تشغيل صفحة إعدادات HP SpareKey، انقر فوق أو اضغط على **Settings** (الإعدادات) في صفحة HP SpareKey (يلزم توفر امتيازات المسؤول).

يمكن أن يحدد المسؤولون الإعدادات التالية:

- حدد الأسئلة التي يتم عرضها على كل مستخدم أثناء إعداد HP SpareKey.
- أضف حتى ثلاثة أسئلة حماية مخصصة لتتم إضافتها إلى القائمة التي يتم عرضها على المستخدمين.
- اختر ما إذا كنت ستتيح للمستخدمين أو لا تتيح لهم كتابة أسئلة الحماية الخاصة بهم.
- حدد أيا من بيئات المصادقة (مصادقة Windows أو المصادقة عند بدء التشغيل) تتيح استخدام HP SpareKey لاسترداد كلمة المرور.

كلمة مرور Windows

يجعل HP Client Security من تغيير كلمة مرور Windows أبسط وأسرع من تغييرها عبر لوحة تحكم Windows.

لتغيير كلمة مرور Windows:

١. من صفحة HP Client Security الرئيسية، انقر فوق أو اضغط على **Windows Password** (كلمة مرور Windows).
٢. أدخل كلمة مرورك الحالية في مربع نص **Current Windows password** (كلمة مرور Windows الحالية).
٣. اكتب كلمة مرور جديدة في مربع نص **New Windows password** (كلمة مرور Windows الجديدة)، ثم اكتبها مرة أخرى في مربع نص **Confirm new password** (تأكيد كلمة المرور الجديدة).
٤. انقر فوق أو اضغط على **Change** (تغيير) لتغيير كلمة المرور الحالية إلى كلمة المرور الجديدة التي أدخلتها على الفور.

أجهزة Bluetooth

في حالة تمكين المسؤول لميزة Bluetooth كوسيلة لتأكيد بيانات اعتماد المصادقة، يمكنك إعداد هاتف يوفر تقنية Bluetooth إلى جانب بيانات الاعتماد الأخرى لتحقيق مزيد من الحماية.

ملاحظة: لا يتاح استخدام سوى أجهزة هاتف Bluetooth.

١. تأكد أنه تم تمكين وظيفة Bluetooth بالكمبيوتر، وأنه تم تعيين هاتف Bluetooth على وضع الاستكشاف. لتوصيل الهاتف، قد تتم مطالبتك بكتابة رمز تم إنشاؤه تلقائيًا في جهاز Bluetooth. وفقًا لإعدادات تكوين جهاز Bluetooth، قد تلزم المقارنة بين رموز الإقران بين الكمبيوتر والهاتف.
٢. لتسجيل الهاتف، حدده ثم انقر فوق أو اضغط على **Enroll** (تسجيل).

للوصول إلى صفحة إعدادات أجهزة Bluetooth في صفحة ١٣ حيث يمكن أن يحدد المسؤول الإعدادات لأجهزة Bluetooth، انقر فوق **Settings** (الإعدادات) (يلزم توفر امتيازات المسؤول).

إعدادات أجهزة Bluetooth

يمكنك أن يحدد المسؤولون الإعدادات التالية التي تتحكم في طريقة واستخدام بيانات اعتماد جهاز Bluetooth:

المصادقة التلقائية

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity** (الاستخدام التلقائي لجهاز Bluetooth المسجل المتصل الخاص بك أثناء التحقق من هويتك) — حدد خانة الاختيار هذه لتتيح للمستخدمين استخدام بيانات اعتماد Bluetooth للمصادقة بدون المطالبة بإجراء من المستخدم أو ألغِ تحديد خانة الاختيار لتعطيل هذا الخيار.

اقتراب Bluetooth

- **Lock computer when your enrolled Bluetooth device moves out of range of your computer** (تأمين الكمبيوتر عندما يتحرك جهاز Bluetooth المسجَّل خارج نطاق الكمبيوتر) — حدد خانة الاختيار هذه لقفل الكمبيوتر عندما يتحرك جهاز Bluetooth الذي كان متصلاً خلال تسجيل الدخول خارج النطاق، أو ألغِ تحديد خانة الاختيار لتعطيل ذلك الخيار.

ملاحظة: يجب أن تتيح وحدة Bluetooth في الكمبيوتر هذه الإمكانية للاستفادة من هذه الميزة.

البطاقات

يمكن أن يتيح HP Client Security استخدام عدد من أنواع بطاقات التعريف المختلفة، وهي بطاقات بلاستيكية صغيرة تتضمن رقاقة كمبيوتر. وتشمل هذه البطاقات البطاقات الذكية والبطاقات غير التلامسية وبطاقات الاقتراب. في حالة توصيل إحدى هذه البطاقات وقارئ البطاقات المناسب بالكمبيوتر مع تثبيت المسؤول لبرنامج التشغيل المقترن من المصنِّع وتمكين المسؤول للبطاقة كوسيلة تأكيد بيانات اعتماد المصادقة، يمكنك استخدام البطاقة كوسيلة تأكيد بيانات اعتماد المصادقة.

بالنسبة إلى البطاقات الذكية، يجب أن يوفر المصنِّع أدوات تثبيت شهادة الحماية وبيانات إدارة رمز PIN والتي تستخدمها HP Client Security في خوارزمية الحماية الخاصة بها. قد يختلف عدد الأحرف المستخدمة كرمز PIN ونوعها. ويجب أن يهيئ المسؤول البطاقة الذكية قبل إمكانية استخدامها.

يتيح HP Client Security استخدام تنسيقات البطاقات الذكية التالية:

- CSP
- PKCS11

يتيح HP Client Security استخدام أنواع البطاقات غير التلامسية التالية:

- بطاقات ذاكرة HID iCLASS غير التلامسية
- بطاقات ذاكرة MiFare Classic 1k و4k غير التلامسية، وبطاقات الذاكرة الصغيرة

يتيح HP Client Security استخدام بطاقات الاقتراب التالية:

- بطاقات اقتراب HID

لتسجيل بطاقة ذكية:

١. أدخل البطاقة في قارئ البطاقة الذكية المتصل.

٢. بعد التعرف على البطاقة، أدخل رمز PIN للبطاقة، ثم انقر فوق أو اضغط على **Enroll** (تسجيل).

لتغيير رمز PIN لبطاقة ذكية:

١. أدخل البطاقة في قارئ البطاقة الذكية المتصل.

٢. بعد التعرف على البطاقة، أدخل رمز PIN للبطاقة، ثم انقر فوق أو اضغط على **Authenticate** (مصادقة).

٣. انقر فوق أو اضغط على **Change PIN** (تغيير رمز PIN)، ثم أدخل رمز PIN الجديد.

لتسجيل بطاقة غير تلامسية أو بطاقة اقتراب:

١. ضع البطاقة في القارئ المناسب أو بالقرب الشديد منه.

٢. بعد التعرف على البطاقة، انقر فوق أو اضغط على **Enroll** (تسجيل).

لحذف بطاقة مسجلة:

١. ضع البطاقة في القارئ.

٢. بالنسبة إلى البطاقات الذكية فقط، أدخل رمز PIN المعيّن للبطاقة، ثم انقر فوق أو اضغط على **Authenticate** (مصادقة).

٣. انقر فوق أو اضغط على **Delete** (حذف).

بمجرد تسجيل البطاقة، يتم عرض تفاصيل حول البطاقة ضمن **Enrolled Cards** (البطاقات المسجلة). وفي حالة حذف بطاقة، تتم إزالتها من القائمة.

للوصول إلى إعدادات بطاقة الاقتراب والبطاقة غير التلامسية والبطاقة الذكية، حيث يمكن أن يحدد المسؤولون الإعدادات المتعلقة ببيانات اعتماد البطاقة، انقر فوق أو اضغط على **Settings** (الإعدادات) (يلزم توفر امتيازات المسؤول).

إعدادات بطاقة الاقتراب والبطاقة غير التلامسية والبطاقة الذكية

للوصول إلى إعدادات بطاقة ما، انقر فوق أو اضغط على البطاقة الموجودة في القائمة، ثم انقر فوق أو اضغط على السهم الذي يظهر.

لتغيير رمز PIN لبطاقة ذكية:

١. ضع البطاقة في القارئ.

٢. أدخل رمز PIN المعيّن للبطاقة، ثم انقر فوق أو اضغط على **Continue** (متابعة).

٣. أدخل رمز PIN الجديد وأكده، ثم انقر فوق أو اضغط على **Continue** (متابعة).

لتهيئة رمز PIN لبطاقة ذكية:

١. ضع البطاقة في القارئ.

٢. أدخل رمز PIN المعيّن للبطاقة، ثم انقر فوق أو اضغط على **Continue** (متابعة).

٣. أدخل رمز PIN الجديد وأكده، ثم انقر فوق أو اضغط على **Continue** (متابعة).

٤. انقر فوق أو اضغط على **Yes** (نعم) لتأكيد التهيئة.

لمسح بيانات البطاقة:

١. ضع البطاقة في القارئ.

٢. أدخل رمز PIN المعيّن للبطاقة (للبطاقات الذكية فقط)، ثم انقر فوق أو اضغط على **Continue** (متابعة).

٣. انقر فوق أو اضغط على **Yes** (نعم) لتأكيد الحذف.

رمز PIN

في حالة تمكين المسؤول لرمز PIN كوسيلة لتأكيد بيانات اعتماد المصادقة، يمكنك إعداد رمز PIN إلى جانب بيانات الاعتماد الأخرى لتحقيق مزيد من الحماية.

لإعداد رمز PIN جديد:

▲ أدخل رمز PIN وأعد إدخاله لتأكيده، ثم انقر فوق أو اضغط على **Apply** (تطبيق).

لحذف رمز PIN:

▲ انقر فوق أو اضغط على **Delete** (حذف)، ثم انقر فوق أو اضغط على **Yes** (نعم) للتأكيد.

للوصول إلى إعدادات رمز PIN، حيث يمكن أن يحدد المسؤولون الإعدادات المتعلقة ببيانات اعتماد رمز PIN، انقر فوق أو اضغط على **Settings** (الإعدادات) (يلزم توفر امتيازات المسؤول).

إعدادات رمز PIN

في صفحة إعدادات PIN، يمكنك تحديد أدنى وأقصى أطوال مقبولة لبيانات اعتماد رمز PIN.

RSA SecurID

في حالة تمكين المسؤول لـ RSA كوسيلة لتأكيد بيانات اعتماد المصادقة، وتحققت الشروط التالية، يمكنك تسجيل بيانات اعتماد RSA SecurID أو حذفها.

ملاحظة: يلزم القيام بالإعداد الصحيح.

- يجب أن يكون تم إنشاء حساب المستخدم على خادم RSA.
- يجب أن يكون تم ربط رمز RSA SecurID المميز المعّين للمستخدم والكمبيوتر بمجال خادم RSA.
- يتم تثبيت برنامج SecurID على الكمبيوتر.
- يتوفر اتصال بخادم RSA الذي تم تكوينه بشكل صحيح.

لتسجيل بيانات اعتماد RSA SecurID:

▲ أدخل اسم مستخدم RSA SecurID ورمز المرور الخاص بك (رمز RSA SecurID Token المميز أو رمز PIN+Token، على حسب بيئة العمل)، ثم انقر فوق أو اضغط على **Apply** (تطبيق).

فور التسجيل الناجح، يتم عرض الرسالة "Your RSA SecurID credential has been successfully enrolled" (تم تسجيل بيانات اعتماد RSA SecurID الخاصة بك بنجاح) ويتم تمكين زر الحذف.

لحذف بيانات اعتماد RSA SecurID:

▲ انقر فوق **Delete** (حذف)، ثم حدد **Yes** (نعم) بمربع الحوار المنبثق الذي يطرح السؤال: "Are you sure you want to delete your RSA SecurID credential?" (هل تريد بالتأكيد حذف بيانات اعتماد RSA SecurID الخاصة بك؟)

Password Manager

يصبح تسجيل الدخول إلى مواقع الويب والتطبيقات أسهل وأكثر أمانًا عند استخدام Password Manager. ويمكنك إنشاء كلمات مرور أقوى لا تضطر إلى كتابتها أو حفظها، ثم تسجيل الدخول بسهولة وبسرعة من خلال بصمة الإصبع أو البطاقة الذكية أو بطاقة الاقتراب أو البطاقة غير التلامسية أو هاتف يعمل بتقنية Bluetooth أو رمز PIN أو بيانات اعتماد RSA أو كلمة مرور Windows.

ملاحظة: نظرًا للبنية المتغيرة باستمرار لشاشات تسجيل الدخول على الويب، ربما يتعذر على تطبيق Password Manager إتاحة استخدام جميع مواقع الويب في جميع الأوقات.

يتيح تطبيق Password Manager الخيارات التالية:

صفحة Password Manager

- انقر فوق أو اضغط على حساب ما لبدء تشغيل صفحة ويب أو تطبيق وتسجيل الدخول تلقائيًا.
- استخدم الفئات لتنظيم حساباتك.

قوة كلمة المرور

- ألقِ نظرة سريعة لتحديد ما إذا كانت أي من كلمات المرور تمثل خطرًا أمنيًا.
- عند إضافة بيانات تسجيل الدخول، تحقق من قوة كلمات المرور المختلفة المستخدمة لمواقع الويب والتطبيقات.
- يتم توضيح قوة كلمة المرور بمؤشرات حالة حمراء أو صفراء أو خضراء.

يتم عرض أيقونة **Password Manager** في الجانب الأيسر العلوي من صفحة الويب أو شاشة تسجيل الدخول إلى التطبيق. إذا لم يتم إنشاء حساب تسجيل الدخول لموقع الويب أو التطبيق ذلك بعد، فسيتم عرض علامة زائد على الأيقونة.

▲ انقر فوق أو اضغط على أيقونة **Password Manager** لعرض قائمة السياق حيث يمكنك الاختيار من بين الخيارات التالية:

- إضافة [somedomain.com] إلى تطبيق Password Manager
- فتح Password Manager

- إعدادات الأيقونة
- تعليمات

بالنسبة إلى صفحات الويب أو البرامج حيث لم يتم إنشاء حساب تسجيل الدخول بعد

يتم عرض الخيارات التالية في قائمة السياق:

- **Add [somedomain.com] to the Password Manager** (إضافة [somedomain.com] إلى Password Manager) — لإتاحة إضافة بيانات تسجيل الدخول لشاشة تسجيل الدخول الحالية.
- **Open Password Manager** (فتح Password Manager) — لبدء تشغيل تطبيق Password Manager.
- **Icon Settings** (إعدادات الأيقونة) — لإتاحة تحديد الحالات التي يتم فيها عرض أيقونة **Password Manager**.
- **Help** (تعليمات) — لعرض تعليمات HP Client Security.

بالنسبة إلى صفحات الويب أو البرامج حيث تم إنشاء حساب تسجيل الدخول بالفعل

يتم عرض الخيارات التالية في قائمة السياق:

- **Fill in logon data** (ملء بيانات تسجيل الدخول) — لعرض صفحة **Verify your identity** (التحقق من هويتك). إذا تمت المصادقة بنجاح، يتم وضع بيانات تسجيل الدخول في حقول تسجيل الدخول، ثم يتم إرسال الصفحة (في حالة تحديد الإرسال عند إنشاء حساب تسجيل الدخول أو في آخر مرة تم تحريره فيها).
- **Edit Logon** (تحرير حساب تسجيل الدخول) — يتيح لك تحرير بيانات تسجيل الدخول إلى موقع الويب هذا.
- **Add Logon** (إضافة حساب تسجيل الدخول) — لإتاحة إضافة حساب إلى Password Manager.
- **Open Password Manager** (فتح Password Manager) — لبدء تشغيل تطبيق Password Manager.
- **Help** (تعليمات) — لعرض تعليمات HP Client Security.

ملاحظة: ربما هيأ مسؤول هذا الكمبيوتر HP Client Security لطلب أكثر من مجموعة واحدة من بيانات الاعتماد عند التحقق من هويتك.

إضافة حسابات تسجيل الدخول

يمكنك بسهولة إضافة حساب تسجيل الدخول إلى موقع ويب أو برنامج بإدخال معلومات تسجيل الدخول مرة واحدة. وبعد تلك المرة، سيدخل تطبيق Password Manager المعلومات تلقائيًا نيابة عنك. ويمكنك استخدام حسابات تسجيل الدخول هذه بعد الاستعراض إلى موقع الويب أو البرنامج.

لإضافة حساب لتسجيل الدخول:

١. افتح شاشة تسجيل الدخول لموقع الويب أو البرنامج.

٢. انقر فوق أو اضغط على أيقونة **Password Manager**، ثم انقر فوق أو اضغط على أي مما يلي استنادًا إلى ما إذا كانت شاشة تسجيل الدخول هي لموقع ويب أو لبرنامج:

- بالنسبة إلى موقع الويب، انقر فوق أو اضغط على **Add [domain name] to Password Manager** (إضافة [اسم المجال] إلى Password Manager).
- في حالة البرنامج، انقر فوق أو اضغط على **Add this logon screen to Password Manager** (إضافة شاشة تسجيل الدخول هذه إلى Password Manager).

٣. أدخل بيانات تسجيل الدخول. يتم تمييز حقول تسجيل الدخول على الشاشة والحقول المناظرة في مربع الحوار من خلال حافة برتقالية عريضة.

أ. لملء حقل تسجيل الدخول بأحد الخيارات المُعدَّة مسبقًا، انقر فوق أو اضغط على الأسهم الموجودة على يمين الحقل.

ب. لعرض كلمة المرور لحساب تسجيل الدخول هذا، انقر فوق أو اضغط على **Show password** (إظهار كلمة المرور).

ج. لملء حقول تسجيل الدخول، بدون إرسالها، ألغِ تحديد خانة الاختيار **Automatically submit logon data** (إرسال بيانات تسجيل الدخول تلقائيًا).

د. انقر فوق أو اضغط على **OK** (موافق) لتحديد طريقة المصادقة التي ترغب في استخدامها (بصمات الأصابع أو البطاقة الذكية أو بطاقة الاقتراب أو البطاقة غير التلامسية أو هاتف بتقنية Bluetooth أو رمز PIN أو كلمة المرور)، ثم سجل الدخول باستخدام طريقة المصادقة المحددة.

تتم إزالة علامة الزائد من أيقونة **Password Manager** لإعلامك بأنه تم إنشاء حساب تسجيل الدخول.

ه. إذا لم يكتشف تطبيق Password Manager حقول تسجيل الدخول، فانقر فوق أو اضغط على **More fields** (المزيد من الحقول).

- حدد خانة الاختيار لكل مجال يلزم لتسجيل الدخول، أو ألغِ تحديد خانة الاختيار لأي حقول غير مطلوبة لتسجيل الدخول.
- انقر فوق أو اضغط على **Close** (إغلاق).

في كل مرة تصل فيها إلى موقع الويب ذلك أو تفتح ذلك البرنامج، يتم عرض أيقونة **Password Manager** في الجزء الأيسر العلوي من موقع الويب أو شاشة تسجيل الدخول إلى التطبيق، مما يدل على إمكانية استخدامك لبيانات الاعتماد المسجلة لتسجيل الدخول.

تحرير حسابات تسجيل الدخول

لتحرير حساب لتسجيل الدخول:

١. افتح شاشة تسجيل الدخول لموقع الويب أو البرنامج.

٢. لعرض مربع حوار حيث يمكنك تحرير معلومات تسجل الدخول، انقر فوق أو اضغط على أيقونة **Password Manager**، ثم انقر فوق أو اضغط على **Edit Logon** (تحرير حساب تسجيل الدخول).

يتم تمييز حقول تسجيل الدخول على الشاشة والحقول المناظرة في مربع الحوار من خلال حافة برتقالية عريضة.

يمكنك أيضًا تحرير معلومات الحساب من داخل صفحة Password Manager بالنقر فوق أو الضغط على حساب تسجيل الدخول لعرض خيارات التحرير، ثم تحديد **Edit** (تحرير).

٣. حرر معلومات تسجيل دخولك.

- لتحرير **Account name** (اسم الحساب)، أدخل اسمًا جديدًا في الحقل.
- لإضافة أو تحرير اسم **Category** (الفئة)، أدخل الاسم أو عدّله في حقل **Category** (الفئة).
- لتحديد حقل تسجيل دخول **Username** (اسم المستخدم) ذي الخيارات المُعدَّة مسبقًا، انقر فوق أو اضغط على السهم لأسفل على يمين الحقل.

تتوفر الخيارات المُعدَّة مسبقًا فقط عند تحرير حساب تسجيل الدخول من الأمر Edit (تحرير) في قائمة سياق أيقونة Password Manager.

- لتحديد حقل تسجيل دخول **Password** (كلمة المرور) ذي الخيارات المُعدَّة مسبقًا، انقر فوق أو اضغط على السهم لأسفل على يمين الحقل.

تتوفر الخيارات المُعدَّة مسبقًا فقط عند تحرير حساب تسجيل الدخول من الأمر Edit (تحرير) في قائمة سياق أيقونة Password Manager.

- لإضافة حقول إضافية من الشاشة إلى حساب تسجيل دخولك، انقر فوق أو اضغط على **More fields** (المزيد من الحقول).
- لعرض كلمة المرور لحساب تسجيل الدخول هذا، انقر فوق أو اضغط على أيقونة **Show password** (إظهار كلمة المرور).
- لملء حقول تسجيل الدخول، بدون إرسالها، ألغِ تحديد خانة الاختيار **Automatically submit logon data** (إرسال بيانات تسجيل الدخول تلقائيًا).
- لتحديد أنه تم اكتشاف كلمة مرور حساب تسجيل الدخول هذا، حدد خانة الاختيار **This password is compromised** (كلمة المرور هذه تم اكتشافها).

بعد حفظ التغييرات، سيتم أيضًا تحديد جميع حسابات تسجيل الدخول الأخرى التي تشترك في كلمة المرور نفسها على أنه تم اكتشافها. وعندئذٍ يمكنك الانتقال إلى كل حساب متأثر وتغيير كلمات المرور حسب الضرورة.

٤. انقر فوق أو اضغط على **OK** (موافق).

استخدام قائمة الروابط السريعة لتطبيق Password Manager

يوفر تطبيق Password Manager طريقة سريعة وسهلة لبدء تشغيل مواقع الويب والبرامج التي تم إنشاء حسابات تسجيل دخول لها. انقر نقرًا مزدوجًا أو اضغط ضغطًا مزدوجًا على حساب تسجيل الدخول إلى برنامج أو موقع ويب من قائمة **Password Manager Quick Links** (الروابط السريعة لتطبيق Password Manager)، أو من صفحة Password Manager داخل HP Client Security، لفتح شاشة تسجيل الدخول، ثم املأ بيانات تسجيل الدخول.

في حالة إنشاء حساب لتسجيل الدخول، فإنه تتم إضافته تلقائيًا إلى قائمة **Quick Links** (الروابط السريعة) في تطبيق Password Manager.

لعرض قائمة **Quick Links** (الروابط السريعة):

- اضغط على مجموعة المفاتيح السريعة الخاصة بتطبيق **Password Manager** (Ctrl+مفتاح Windows+h هو إعداد المصنع). لتغيير مجموعة مفاتيح التشغيل السريع، من صفحة HP Client Security الرئيسية، انقر فوق **Password Manager**، ثم انقر فوق أو اضغط على **Settings** (الإعدادات).

ترتيب حسابات تسجيل الدخول في فئات

أنشئ فئة أو أكثر للحفاظ على تنظيم حسابات تسجيل الدخول.

لضم حساب تسجيل الدخول إلى فئة ما:

١. من صفحة HP Client Security الرئيسية، انقر فوق أو اضغط على **Password Manager**.

٢. انقر فوق أو اضغط على أحد الإدخالات بالحساب، ثم انقر فوق أو اضغط على **Edit** (تحرير).

٣. في حقل **Category** (الفئة)، أدخل اسم فئة.

٤. انقر فوق أو اضغط على **Save** (حفظ).

لإزالة حساب من فئة ما:

١. من صفحة HP Client Security الرئيسية، انقر فوق أو اضغط على **Password Manager**.

٢. انقر فوق أو اضغط على أحد الإدخالات بالحساب، ثم انقر فوق أو اضغط على **Edit** (تحرير).

٣. في حقل **Category** (الفئة)، امح اسم الفئة.

٤. انقر فوق أو اضغط على **Save** (حفظ).

لإعادة تسمية فئة ما:

١. من صفحة HP Client Security الرئيسية، انقر فوق أو اضغط على **Password Manager**.

٢. انقر فوق أو اضغط على أحد الإدخالات بالحساب، ثم انقر فوق أو اضغط على **Edit** (تحرير).

٣. في حقل **Category** (الفئة)، غيّر اسم الفئة.

٤. انقر فوق أو اضغط على **Save** (حفظ).

إدارة حسابات تسجيل الدخول

ييسر تطبيق Password Manager من إدارة معلومات تسجيل الدخول لأسماء المستخدمين وكلمات المرور وحسابات تسجيل الدخول المتعددة من موقع مركزي واحد.

ويتم عرض حسابات تسجيل الدخول في صفحة Password Manager.

لإدارة حسابات تسجيل الدخول:

١. من صفحة HP Client Security الرئيسية، انقر فوق أو اضغط على **Password Manager**.

٢. انقر فوق أو اضغط على حساب تسجيل دخول حالي، ثم حدد أحد الخيارات التالية، ثم اتبع الإرشادات الظاهرة على الشاشة:

- **Edit** (تحرير) — لتحرير حساب تسجيل الدخول. للحصول على مزيد من المعلومات، انظر تحرير حسابات تسجيل الدخول في صفحة ١٨.
- **Log in** — (تسجيل الدخول) لتسجيل الدخول إلى الحساب المحدد.
- **Delete** — (حذف) لحذف بيانات تسجيل الدخول إلى الحساب المحدد.

لإضافة حساب تسجيل دخول إضافي إلى موقع ويب أو برنامج:

١. افتح شاشة تسجيل الدخول لموقع الويب أو البرنامج.

٢. انقر فوق أو اضغط على أيقونة **Password Manager** لعرض قائمة السياق للتطبيق.

٣. انقر فوق أو اضغط على **Add Logon** (إضافة حساب تسجيل الدخول)، ثم اتبع الإرشادات الظاهرة على الشاشة.

تقييم قوة كلمة المرور

يعد استخدام كلمات مرور قوية لتسجيل الدخول إلى مواقع الويب والبرامج أحد الجوانب المهمة لحماية هويتك.

ويسر تطبيق Password Manager من مراقبة عملية الحماية وتحسينها من خلال التحليل الفوري والتلقائي لقوة كل كلمة من كلمات المرور المستخدمة لتسجيل الدخول إلى مواقع الويب والبرامج الخاصة بك.

أثناء إدخال كلمة مرور خلال إنشاء بيانات تسجيل دخول Password Manager إلى حساب ما، يتم عرض شريط ملون أسفل كلمة المرور للدلالة على قوة كلمة المرور. تدل الألوان على القيم التالية:

- **الأحمر** — ضعيفة
- **الأصفر** — مقبولة
- **الأخضر** — قوية

إعدادات أيقونة Password Manager

يحاول تطبيق Password Manager تحديد شاشات تسجيل الدخول إلى مواقع الويب والبرامج. وعندما يكتشف شاشة تسجيل دخول لم ينشئ المستخدم حساب تسجيل دخول لها، يطالب Password Manager بإضافة حساب تسجيل الدخول للشاشة من خلال عرض أيقونة **Password Manager** بالإضافة إلى علامة زائد.

١. انقر فوق أو اضغط على الأيقونة، ثم انقر فوق أو اضغط على **Icon Settings** (إعدادات الأيقونة) لتخصيص كيفية تعامل تطبيق Password Manager مع مواقع تسجيل الدخول المحتملة.

- **Prompt to add logons for logon screens** (المطالبة بإضافة حسابات تسجيل الدخول لشاشات تسجيل الدخول) — انقر فوق أو اضغط على هذا الخيار ليطالبك Password Manager بإضافة حساب تسجيل الدخول في حالة عرض شاشة تسجيل دخول لم يتم بالفعل إعداد حساب تسجيل الدخول لها.
- **Exclude this screen** (استثناء هذه الشاشة) — حدد خانة الاختيار هذه حتى لا يطالبك Password Manager مرة أخرى بإضافة حساب تسجيل الدخول لشاشة تسجيل الدخول هذه.
- **Do not prompt to add logons for logon screens** (عدم المطالبة بإضافة حسابات تسجيل الدخول لشاشات تسجيل الدخول) — حدد زر الخيار.

٢. لإضافة حساب لتسجيل الدخول إلى شاشة تم استثناؤها مسبقًا:

أ. سجل الدخول إلى موقع الويب الذي تم استثناؤه مسبقًا.

ب. لتجعل تطبيق Password Manager يتذكر كلمة المرور لهذا الموقع، انقر فوق أو اضغط على **Remember** (تذكر) في مربع الحوار المنبثق لحفظ كلمة المرور وإنشاء حساب تسجيل الدخول للشاشة.

٣. للوصول إلى إعدادات Password Manager الإضافية، انقر فوق أو اضغط على أيقونة Password Manager، وانقر فوق أو اضغط على **Open Password Manager** (فتح Password Manager)، ثم انقر فوق أو اضغط على **Settings** (الإعدادات) في صفحة Password Manager.

استيراد وتصدير حسابات تسجيل الدخول

في صفحة استيراد وتصدير HP Password Manager، يمكنك استيراد حسابات تسجيل الدخول التي يتم حفظها بواسطة مستعرضات الويب على الكمبيوتر. ويمكنك أيضًا استيراد البيانات من ملف النسخة الاحتياطية لبرنامج HP Client Security وتصدير البيانات إلى ذلك الملف.

▲ لبدء تشغيل صفحة الاستيراد والتصدير، انقر فوق أو اضغط على **Import and export** (استيراد وتصدير) في صفحة Password Manager.

لاستيراد كلمات المرور من مستعرض:

١. انقر فوق أو اضغط على المستعرض الذي تريد استيراد كلمات المرور منه (يتم عرض المستعرضات التي تم تثبيتها فقط).

٢. ألغِ تحديد خانة الاختيار لأية حسابات لا تريد استيراد كلمات المرور لها.

٣. انقر فوق أو اضغط على **Import** (استيراد).

يمكن تنفيذ عملية استيراد البيانات من ملف النسخة الاحتياطية لبرنامج HP Client Security أو تصدير البيانات إليه من خلال الروابط المقترنة (أسفل **Other Options** (خيارات أخرى)) في صفحة الاستيراد والتصدير.

ملاحظة: تستورد هذه الميزة وتصدر بيانات Password Manager فقط. للحصول على معلومات حول النسخ الاحتياطي لبيانات HP Client Security الإضافية واستعادتها، انظر النسخ الاحتياطي للبيانات واستعادتها في صفحة ٢٥.

لاستيراد البيانات من ملف النسخة الاحتياطية لبرنامج HP Client Security:

١. من صفحة استيراد وتصدير HP Password Manager، انقر فوق أو اضغط على **Import data from an HP Client Security backup file** (استيراد البيانات من ملف النسخة الاحتياطية لبرنامج HP Client Security).

٢. أكد هويتك.

٣. حدد ملف النسخة الاحتياطية الذي تم إنشاؤه مسبقًا أو أدخل المسار في الحقل المتاح، ثم انقر فوق أو اضغط على **Browse** (استعراض).

٤. أدخل كلمة المرور المستخدمة لحماية الملف، ثم انقر فوق أو اضغط على **Next** (التالي).

٥. انقر فوق أو اضغط على **Restore** (استعادة).

لتصدير البيانات إلى ملف النسخة الاحتياطية لبرنامج HP Client Security:

١. من صفحة استيراد وتصدير HP Password Manager، انقر فوق أو اضغط على **Export data from an HP Client Security backup file** (تصدير البيانات من ملف النسخة الاحتياطية لبرنامج HP Client Security).

٢. أكّد هويتك، ثم انقر فوق أو اضغط على **Next** (التالي).

٣. أدخل اسمًا لملف النسخة الاحتياطية. بشكل افتراضي، يتم حفظ الملف بمجلد المستندات. لتحديد موقع مختلف، انقر فوق أو اضغط على **Browse** (استعراض).

٤. أدخل كلمة مرور وأكدها لحماية الملف، ثم انقر فوق أو اضغط على **Save** (حفظ).

الإعدادات

يمكنك تحديد الإعدادات اللازمة لإضفاء الطابع الشخصي على Password Manager:

- **Prompt to add logons for logon screens** (المطالبة بإضافة حسابات تسجيل الدخول لشاشات تسجيل الدخول) — يتم عرض أيقونة **Password Manager** بالإضافة إلى علامة زائد عند اكتشاف شاشة تسجيل دخول إلى موقع ويب أو برنامج، مما يدل على أنه يمكنك إضافة حساب تسجيل الدخول إلى هذه الشاشة إلى قائمة **Logons** (حسابات تسجيل الدخول).

  لتعطيل هذه الميزة، ألغِ تحديد خانة الاختيار بجوار **Prompt to add logons for logon screens** (المطالبة بإضافة حسابات تسجيل الدخول لشاشات تسجيل الدخول).

- **Open Password Manager with Ctrl+Win+h** — (فتح Password Manager بمجموعة المفاتيح Ctrl+Win+h) وهو مفتاح التشغيل السريع الافتراضي الذي يفتح قائمة **Password Manager Quick Links** (ارتباطات Password Manager السريعة) وهو Ctrl+مفتاح Windows+h.

  لتغيير مفتاح التشغيل السريع، انقر فوق أو اضغط على هذا الخيار، ثم أدخل مجموعة مفاتيح جديدة. يمكن أن تشمل المجموعات واحدًا أو أكثر مما يلي: ctrl أو alt أو shift وأي مفتاح أبجدي أو رقمي.

  لا يمكن استخدام مجموعات الأحرف المحجوزة لنظام Windows أو لتطبيقات Windows.

- لإعادة الإعدادات إلى القيم الافتراضية للمصنع، انقر فوق أو اضغط على **Restore defaults** (استعادة الافتراضيات).

الإعدادات المتقدمة

يمكن للمسؤولين الوصول إلى الخيارات التالية من خلال تحديد أيقونة **Gear** (الترس) (الإعدادات) في صفحة HP Client Security الرئيسية.

- **Administrator Policies** (سياسات المسؤول) — لإتاحة تكوين سياسات تسجيل الدخول والجلسات للمسؤولين.
- **Standard User Policies** (سياسات المستخدم القياسي) — لإتاحة تكوين سياسات تسجيل الدخول والجلسات للمستخدمين القياسيين.
- **Security Features** (ميزات الحماية) — لإتاحة زيادة مستوى حماية الكمبيوتر بواسطة حماية حساب Windows باستخدام إجراءات المصادقة الفعالة و/أو تمكين المصادقة قبل بدء تشغيل Windows.
- **Users** (المستخدمون) — لإتاحة إدارة المستخدمين وبيانات اعتمادهم.
- **My Policies** (سياساتي) — لإتاحة مراجعة سياسات المصادقة وحالة التسجيل.
- **Backup and Restore** (النسخ الاحتياطي والاستعادة) — لإتاحة نسخ بيانات HP Client Security أو استعادتها.
- **About HP Client Security** (نبذة عن HP Client Security) — لعرض معلومات الإصدار الخاصة ببرنامج HP Client Security.

سياسات المسؤول

يمكنك تكوين سياسات تسجيل الدخول والجلسات لمسؤولي هذا الكمبيوتر. وتتحكم سياسات تسجيل الدخول المحددة هنا في بيانات الاعتماد اللازمة لمسؤول محلي ليتمكن من تسجيل الدخول إلى Windows. كما تتحكم سياسات الجلسات المحددة هنا في بيانات الاعتماد اللازمة لمسؤول محلي للتحقق من الهوية داخل جلسة عمل Windows.

بصورة افتراضية، يتم فرض جميع السياسات الجديدة أو التي تم تغييرها على الفور بعد النقر فوق أو الضغط على **Apply** (تطبيق).

لإضافة سياسة جديدة:

١. من صفحة HP Client Security الرئيسية، انقر فوق أو اضغط على أيقونة **Gear** (الترس).

٢. في صفحة الإعدادات المتقدمة، انقر فوق أو اضغط على **Administrator Policies** (سياسات المسؤول).

٣. انقر فوق أو اضغط على **Add new policy** (إضافة سياسة جديدة).

٤. اضغط على الأسهم لأسفل لتحديد بيانات الاعتماد الأساسية والثانوية (الاختيارية) للسياسة الجديدة، ثم انقر فوق أو اضغط على **Add** (إضافة).

٥. انقر فوق **Apply** (تطبيق).

لتأخير فرض سياسة جديدة أو تم تغييرها:

١. انقر فوق أو اضغط على **Enforce this policy immediately** (فرض هذه السياسة على الفور).

٢. حدد **Enforce this policy on the specific date** (فرض هذه السياسة في الموعد المحدد).

٣. أدخل تاريخًا أو استخدم التقويم المنبثق لتحديد تاريخ وجوب فرض هذه السياسة.

٤. إذا كنت تريد ذلك، فحدد موعد تذكير المستخدمين بشأن السياسة الجديدة.

٥. انقر فوق **Apply** (تطبيق).

سياسات المستخدم القياسي

يمكنك تكوين سياسات تسجيل الدخول والجلسات لمستخدمي هذا الكمبيوتر القياسيين. وتتحكم سياسات تسجيل الدخول المحددة هنا في بيانات الاعتماد اللازمة لمستخدم قياسي ليتمكن من تسجيل الدخول إلى Windows. كما تتحكم سياسات الجلسات المحددة هنا في بيانات الاعتماد اللازمة لمستخدم قياسي للتحقق من الهوية داخل جلسة عمل Windows.

بصورة افتراضية، يتم فرض جميع السياسات الجديدة أو التي تم تغييرها على الفور بعد النقر فوق أو الضغط على **Apply** (تطبيق).

لإضافة سياسة جديدة:

١. من صفحة HP Client Security الرئيسية، انقر فوق أو اضغط على أيقونة **Gear** (الترس).

٢. في صفحة الإعدادات المتقدمة، انقر فوق أو اضغط على **Standard User Policies** (سياسات المستخدم القياسي).

٣. انقر فوق أو اضغط على **Add new policy** (إضافة سياسة جديدة).

٤. اضغط على الأسهم لأسفل لتحديد بيانات الاعتماد الأساسية والثانوية (الاختيارية) للسياسة الجديدة، ثم انقر فوق أو اضغط على **Add** (إضافة).

٥. انقر فوق **Apply** (تطبيق).

لتأخير فرض سياسة جديدة أو تم تغييرها:

١. انقر فوق أو اضغط على **Enforce this policy immediately** (فرض هذه السياسة على الفور).

٢. حدد **Enforce this policy on the specific date** (فرض هذه السياسة في الموعد المحدد).

٣. أدخل تاريخًا أو استخدم التقويم المنبثق لتحديد تاريخ وجوب فرض هذه السياسة.

٤. إذا كنت تريد ذلك، فحدد موعد تذكير المستخدمين بشأن السياسة الجديدة.

٥. انقر فوق **Apply** (تطبيق).

ميزات الحماية

يمكنك تمكين ميزات HP Client Security التي تساعد في الحماية ضد الوصول غير المرخص إلى الكمبيوتر.

لإعداد ميزات الحماية:

١. من صفحة HP Client Security الرئيسية، انقر فوق أو اضغط على أيقونة **Gear** (الترس).

٢. في صفحة الإعدادات المتقدمة، انقر فوق أو اضغط على **Security Features** (ميزات الحماية).

٣. مكّن ميزات الحماية من خلال تحديد خانات الاختيار، ثم النقر فوق أو الضغط على **Apply** (تطبيق). كلما حددت ميزات أكثر، كان جهاز الكمبيوتر أكثر حماية.

تنطبق هذه الإعدادات على جميع المستخدمين.

- **Windows Logon Security** (حماية تسجيل الدخول إلى Windows) — لحماية حسابات Windows الخاصة بك من خلال طلب استخدام بيانات اعتماد HP Client Security للدخول.
- **Pre-Boot Security (Power-on authentication)** (حماية ما قبل التمهيد (المصادقة عند بدء التشغيل)) — لحماية الكمبيوتر قبل بدء تشغيل Windows. هذا التحديد غير متاح إذا لم يدعمه نظام BIOS.
- **Allow One Step logon** (السماح بتسجيل الدخول بخطوة واحدة) — يتيح هذا الإعداد تخطي تسجيل الدخول إلى Windows إذا تم إجراء المصادقة مسبقًا عند مستوى المصادقة عند بدء التشغيل أو Drive Encryption.

٤. انقر فوق أو اضغط على **Users** (المستخدمون)، ثم انقر فوق أو اضغط على لوحة المستخدم.

المستخدمون

يمكنك مراقبة مستخدمي HP Client Security لهذا الكمبيوتر وإدارتهم.

لإضافة مستخدم Windows آخر إلى HP Client Security:

١. من صفحة HP Client Security الرئيسية، انقر فوق أو اضغط على أيقونة **Gear** (الترس).

٢. في صفحة الإعدادات المتقدمة، انقر فوق أو اضغط على **Users** (المستخدمون).

٣. انقر فوق أو اضغط على **Add another Windows user to HP Client Security** (إضافة مستخدم Windows آخر إلى HP Client Security).

٤. أدخل اسم المستخدم الذي تريد إضافته، ثم انقر فوق أو اضغط على **OK** (موافق).

٥. أدخل كلمة مرور Windows للمستخدم.

فيتم عرض لوحة للمستخدم المضاف في صفحة المستخدم.

لحذف مستخدم Windows من HP Client Security:

١. من صفحة HP Client Security الرئيسية، انقر فوق أو اضغط على أيقونة **Gear** (الترس).

٢. في صفحة الإعدادات المتقدمة، انقر فوق أو اضغط على **Users** (المستخدمون).

٣. انقر فوق أو اضغط على اسم المستخدم الذي تريد حذفه.

٤. انقر فوق أو اضغط على **Delete User** (حذف المستخدم)، ثم انقر فوق أو اضغط على **Yes** (نعم) للتأكيد.

لعرض ملخص لسياسات تسجيل الدخول والجلسات المفروضة لمستخدم:

▲ انقر فوق أو اضغط على **Users** (المستخدمون)، ثم انقر فوق أو اضغط على لوحة المستخدم.

سياساتي

يمكنك عرض سياسات المصادقة وحالة التسجيل. كما توفر صفحة سياساتي أيضًا روابط لصفحات سياسات المسؤولين وسياسات المستخدم القياسي.

١. من صفحة HP Client Security الرئيسية، انقر فوق أو اضغط على أيقونة **Gear** (الترس).

٢. في صفحة الإعدادات المتقدمة، انقر فوق أو اضغط على **My Policies** (سياساتي).

يتم عرض سياسات تسجيل الدخول والجلسات المفروضة للمستخدم المسجل للدخول حاليًا.

كما توفر صفحة سياساتي روابط إلى سياسات المسؤول في صفحة ٢٣ وسياسات المستخدم القياسي في صفحة ٢٣.

النسخ الاحتياطي للبيانات واستعادتها

يُوصى بنسخ بيانات HP Client Security احتياطيًا بصفة منتظمة. ويعتمد عدد المرات التي تقوم فيها بالنسخ الاحتياطي على عدد مرات تغيير البيانات. على سبيل المثال، إذا كنت تضيف حسابات تسجيل دخول جديدة بصفة يومية، يجب أن تنسخ بياناتك احتياطيًا بصفة يومية.

يمكن أيضًا استخدام عمليات النسخ الاحتياطي لترحيل البيانات من كمبيوتر إلى آخر، وهو ما يسمى بالاستيراد والتصدير.

ملاحظة: لا يتم النسخ الاحتياطي سوى لتطبيق Password Manager من خلال هذه الميزة. بينما يتم نسخ Drive Encryption بطريقة نسخ احتياطي مستقلة. ولا يتم نسخ معلومات مصادقة Device Access Manager وبصمات الأصابع احتياطيًا.

يجب تثبيت HP Client Security على أي كمبيوتر مجهز لاستقبال بيانات منسوخة احتياطيًا قبل استعادة البيانات من ملف النسخ الاحتياطي.

لنسخ بياناتك احتياطيًا:

١. من صفحة HP Client Security الرئيسية، انقر فوق أو اضغط على أيقونة **Gear** (الترس).

٢. في صفحة الإعدادات المتقدمة، انقر فوق أو اضغط على **Administrator Policies** (سياسات المسؤول).

٣. انقر فوق أو اضغط على **Backup and Restore** (النسخ الاحتياطي والاستعادة).

٤. انقر فوق أو اضغط على **Backup** (نسخ احتياطي)، ثم أكّد هويتك.

٥. حدد الوحدة التي تريد تضمينها في النسخ الاحتياطي، ثم انقر فوق أو اضغط على **Next** (التالي).

٦. أدخل اسمًا لملف التخزين. بشكل افتراضي، يتم حفظ الملف بمجلد المستندات. لتحديد موقع مختلف، انقر فوق أو اضغط على **Browse** (استعراض).

٧. أدخل كلمة مرور وأكدها لحماية الملف.

٨. انقر فوق أو اضغط على **Save** (حفظ).

لاستعادة بياناتك:

١. من صفحة HP Client Security الرئيسية، انقر فوق أو اضغط على أيقونة **Gear** (الترس).

٢. في صفحة الإعدادات المتقدمة، انقر فوق أو اضغط على **Administrator Policies** (سياسات المسؤول).

٣. انقر فوق أو اضغط على **Backup and Restore** (النسخ الاحتياطي والاستعادة).

٤. حدد **Restore** (استعادة)، ثم أكّد هويتك.

٥. حدد ملف التخزين الذي تم إنشاؤه سابقًا. أدخل المسار في الحقل المتاح. لتحديد موقع مختلف، انقر فوق أو اضغط على **Browse** (استعراض).

٦. أدخل كلمة المرور المستخدمة لحماية الملف، ثم انقر فوق أو اضغط على **Next** (التالي).

٧. حدد الوحدات التي تريد استعادة بياناتها.

٨. انقر فوق أو اضغط على **Restore** (استعادة).

٥ HP Drive Encryption (طُرز محددة فقط)

يوفر تطبيق HP Drive Encryption حماية كاملة للبيانات من خلال تشفير بياناتك على الكمبيوتر. وعند تنشيط Drive Encryption، يجب تسجيل الدخول من شاشة تسجيل الدخول إلى Drive Encryption، والتي يتم عرضها قبل بدء تشغيل نظام Windows®.

تسمح الشاشة الرئيسية لبرنامج HP Client Security لمسؤولي Windows بتنشيط Drive Encryption ونسخ مفتاح التشفير احتياطيًا وتحديد أو إلغاء تحديد محرك (محركات) القرص أو القسم (الأقسام) لإجراء التشفير. للحصول على مزيد من المعلومات، انظر تعليمات برنامج HP Client Security.

يمكن تنفيذ المهام التالية من خلال Drive Encryption:

- تحديد إعدادات Drive Encryption:
  - تشفير محركات أقراص أو أقسام معينة أو فك تشفيرها باستخدام تشفير البرامج
  - تشفير محركات أقراص معينة ذاتية التشفير أو فك تشفيرها باستخدام تشفير الأجهزة
  - إضافة المزيد من الحماية من خلال تعطيل وضعي السكون والاستعداد لضمان المطالبة دائمًا بمصادقة ما قبل التمهيد في Drive Encryption

ملاحظة: لا يمكن تشفير سوى محركي القرص الثابت الداخلي من نوع SATA والخارجي من نوع eSATA.

- إنشاء مفاتيح النسخ الاحتياطي
- استرداد إمكانية الوصول إلى كمبيوتر مشفر باستخدام مفاتيح النسخ الاحتياطي وHP SpareKey
- تمكين مصادقة ما قبل التمهيد في Drive Encryption باستخدام كلمة مرور أو بصمة إصبع مسجلة أو رمز PIN لبطاقات ذكية محددة

فتح Drive Encryption

يمكن للمسؤولين الوصول إلى Drive Encryption عبر فتح برنامج HP Client Security:

١. من شاشة Start (ابدأ)، انقر فوق أو اضغط على تطبيق **HP Client Security** (في نظام التشغيل Windows 8).

– أو –

من سطح مكتب Windows، انقر نقرًا مزدوجًا فوق أيقونة **HP Client Security** في منطقة الإعلام بأقصى يمين شريط المهام، أو اضغط عليها ضغطًا مزدوجًا.

٢. انقر فوق أو اضغط على أيقونة **Drive Encryption**.

المهام العامة

تنشيط Drive Encryption لمحركات الأقراص الثابتة القياسية

يتم تشفير محركات الأقراص الثابتة القياسية باستخدام تشفير البرامج. اتبع الخطوات التالية لتشفير محرك قرص أو قسم من قرص:

١. ابدأ تشغيل **Drive Encryption**. للحصول على مزيد من المعلومات، انظر فتح Drive Encryption في صفحة ٢٦.

٢. حدد خانة الاختيار الخاص بمحرك القرص أو القسم الذي تريد تشفيره، ثم انقر فوق أو اضغط على **Backup Key** (مفتاح النسخ الاحتياطي).

ملاحظة: للحصول على مستوى أفضل من الحماية، حدد خانة الاختيار **Disable sleep mode for increased security** (تعطيل وضع السكون لمزيد من الحماية). عند تعطيل وضع السكون، لا يوجد أي احتمال على الإطلاق لتخزين بيانات الاعتماد المستخدمة لإلغاء تأمين محرك القرص في الذاكرة.

٣. حدد خيارًا أو أكثر من خيارات النسخ الاحتياطي، ثم انقر فوق أو اضغط على **Backup** (نسخ احتياطي). للحصول على مزيد من المعلومات، انظر النسخ الاحتياطي لمفاتيح التشفير في صفحة ٢٩.

٤. يمكنك متابعة العمل أثناء تنفيذ النسخ الاحتياطي لمفتاح التشفير. لا تُعِد تمهيد الكمبيوتر.

ملاحظة: سيطلب منك إعادة تشغيل الكمبيوتر. بعد إعادة التشغيل، يتم عرض شاشة ما قبل تمهيد Drive Encryption، حيث تُطلب منك المصادقة قبل بدء تشغيل نظام التشغيل Windows.

تم تنشيط Drive Encryption. قد يستغرق تشفير قسم (أقسام) محرك القرص المحدد عدة ساعات، ويعتمد هذا على عدد الأقسام وحجمها.

للحصول على مزيد من المعلومات، انظر تعليمات برنامج HP Client Security.

تنشيط Drive Encryption لمحركات الأقراص ذاتية التشفير

يمكن استخدام تشفير البرامج أو تشفير الأجهزة لتشفير محركات الأقراص ذاتية التشفير المستوفية لمواصفات Trusted Computing Group's OPAL المتعلقة بإدارة محرك القرص ذاتي التشفير. ويتميز تشفير الأجهزة بأنه أسرع بكثير من تشفير البرامج. ولكن لا يمكنك اختيار أقسام محرك القرص التي يراد تشفيرها. ولهذا يتم تشفير كامل محرك القرص، بما في ذلك أية أقسام به.

لتشفير أقسام محددة، يجب استخدام تشفير البرامج. تأكد من إلغاء تحديد خانة الاختيار **Only allow hardware encryption for Self-Encrypting Drives (SEDs)** (السماح بتشفير الأجهزة فقط لمحركات الأقراص ذاتية التشفير).

اتبع هذه الخطوات لتنشيط Drive Encryption بالنسبة لمحركات الأقراص ذاتية التشفير:

١. ابدأ تشغيل **Drive Encryption**. للحصول على مزيد من المعلومات، انظر فتح Drive Encryption في صفحة ٢٦.

٢. حدد خانة الاختيار الخاصة بمحرك القرص الذي تريد تشفيره، ثم انقر فوق أو اضغط على **Backup Key** (مفتاح النسخ الاحتياطي).

ملاحظة: للحصول على مستوى أفضل من الحماية، حدد خانة الاختيار **Disable Sleep Mode for added security** (تعطيل وضع السكون لحماية إضافية). عند تعطيل وضع السكون، لا يوجد أي احتمال على الإطلاق لتخزين بيانات الاعتماد المستخدمة لإلغاء تأمين محرك القرص في الذاكرة.

٣. حدد خيارًا أو أكثر من خيارات النسخ الاحتياطي، ثم انقر فوق أو اضغط على **Backup** (نسخ احتياطي). للحصول على مزيد من المعلومات، انظر النسخ الاحتياطي لمفاتيح التشفير في صفحة ٢٩.

٤. يمكنك متابعة العمل أثناء تنفيذ النسخ الاحتياطي لمفتاح التشفير. لا تُعِد تمهيد الكمبيوتر.

ملاحظة: بالنسبة لمحركات الأقراص ذاتية التشفير، ستتم مطالبتك بإيقاف تشغيل الكمبيوتر.

للحصول على مزيد من المعلومات، انظر تعليمات برنامج HP Client Security.

إلغاء تنشيط Drive Encryption

١. ابدأ تشغيل **Drive Encryption**. للحصول على مزيد من المعلومات، انظر فتح Drive Encryption في صفحة ٢٦.

٢. ألغِ تحديد خانة الاختيار لجميع محركات الأقراص المشفرة، ثم انقر فوق أو اضغط على **Apply** (تطبيق).

سيبدأ حينئذ إلغاء تنشيط Drive Encryption.

ملاحظة: إذا تم استخدام تشفير البرامج، فسيبدأ فك التشفير. قد يستغرق الأمر عدة ساعات، ويعتمد هذا على حجم قسم (أقسام) محرك القرص الثابت المشفر. عند اكتمال فك التشفير، سيتم إلغاء تنشيط Drive Encryption.

إذا تم استخدام تشفير الأجهزة، فسيتم فك تشفير محرك القرص على الفور، وسيتم إلغاء تنشيط Drive Encryption بعد بضع دقائق.

وبمجرد إلغاء تنشيط Drive Encryption، ستتم مطالبتك بإيقاف تشغيل الكمبيوتر في حالة التشفير بالأجهزة، أو إعادة تشغيله في حالة التشفير بالبرامج.

تسجيل الدخول بعد تنشيط Drive Encryption

عند تشغيل الكمبيوتر، بعد تنشيط Drive Encryption وتسجيل حساب المستخدم الخاص بك، يجب أن تسجل دخولك في شاشة تسجيل الدخول إلى Drive Encryption:

ملاحظة: عند تنبيه الكمبيوتر من وضع السكون أو الاستعداد، لا يتم عرض مطالبة مصادقة ما قبل التمهيد في Drive Encryption لكل من تشفير البرامج أو تشفير الأجهزة. يوفر تشفير الأجهزة خيار **Disable sleep mode for increased security** (تعطيل وضع السكون لمزيد من الحماية) الذي يمنع - عند تمكينه - تنشيط وضع السكون أو وضع الاستعداد.

عند تنبيه الكمبيوتر من وضع الإسبات، سيتم عرض مطالبة مصادقة ما قبل التمهيد في Drive Encryption لكلّ من تشفير البرامج وتشفير الأجهزة.

ملاحظة: إذا كان مسؤول Windows قد مكّن خيار BIOS Pre-boot Security (حماية ما قبل التمهيد في BIOS) في برنامج HP Client Security وإذا تم تمكين خيار One-Step Logon (تسجيل الدخول بخطوة واحدة) (افتراضيًا)، يمكنك تسجيل الدخول إلى الكمبيوتر فور المصادقة في BIOS Pre-boot (ما قبل التمهيد في BIOS) دون الحاجة إلى إعادة المصادقة في شاشة تسجيل الدخول إلى Drive Encryption.

تسجيل الدخول في حالة المستخدم الوحيد:

- في صفحة **Logon** (تسجيل الدخول)، أدخل كلمة مرور Windows أو رمز PIN للبطاقة الذكية أو SpareKey أو مرر إصبعًا مسجلاً.

تسجيل الدخول في حالة المستخدمين المتعددين:

١. في صفحة **Select user to logon** (تحديد مستخدم لتسجيل الدخول)، حدد المستخدم المراد تسجيل دخوله من القائمة المنسدلة، ثم انقر فوق أو اضغط على **Next** (التالي).

٢. في صفحة **Logon** (تسجيل الدخول)، أدخل كلمة مرور Windows أو رمز PIN للبطاقة الذكية أو مرر إصبعًا مسجلاً.

ملاحظة: البطاقات الذكية التالية يتاح استخدامها:

البطاقات الذكية المتاح استخدامها

- Gemalto Cyberflex Access 64k V2c

ملاحظة: إذا تم استخدام مفتاح الاسترداد لتسجيل الدخول في شاشة تسجيل الدخول إلى Drive Encryption، فسيتطلب الأمر بيانات اعتماد إضافية عند تسجيل الدخول إلى Windows للوصول إلى حسابات المستخدمين.

تشفير محركات أقراص ثابتة إضافية

يوصى بشدة باستخدام HP Drive Encryption لحماية البيانات عبر تشفير محرك القرص الثابت لديك. بعد التنشيط، يمكن تشفير أية محركات أقراص ثابتة أو أقسام إضافية باتباع هذه الخطوات:

١. ابدأ تشغيل **Drive Encryption**. للحصول على مزيد من المعلومات، انظر فتح Drive Encryption في صفحة ٢٦.

٢. بالنسبة لمحركات الأقراص التي يتم تشفيرها بالبرامج، حدد أقسام محرك الأقراص التي يراد تشفيرها.

ملاحظة: ينطبق هذا الأمر كذلك على سيناريو محركات الأقراص المختلطة الذي يتوافر فيه محرك قرص ثابت قياسي أو أكثر ومحرك قرص ثابت ذاتي التشفير أو أكثر.

– أو –

- بالنسبة لمحركات الأقراص المشفرة بالأجهزة، حدد محرك (محركات) الأقراص الإضافي المراد تشفيره.

المهام المتقدمة

إدارة Drive Encryption (مهمة المسؤول)

يمكن للمسؤولين استخدام Drive Encryption لعرض حالة تشفير جميع محركات الأقراص الثابتة بالكمبيوتر (غير مشفر أو مشفر) وتغييرها.

- إذا كانت الحالة Enabled (ممكن)، فقد تم تنشيط Drive Encryption وتكوينه. يكون محرك القرص في واحدة من الحالات التالية:

تشفير البرامج

- Not Encrypted (غير مشفر)
- Encrypted (مشفر)
- Encrypting (جارٍ التشفير)
- Decrypting (جارٍ فك التشفير)

تشفير الأجهزة

- Encrypted (مشفر)
- Not Encrypted (غير مشفر) (لمحركات الأقراص الإضافية)

تشفير أو فك تشفير أقسام محرك قرص معينة (تشفير البرامج فقط)

يمكن للمسؤولين استخدام Drive Encryption في تشفير قسم أو أكثر من أقسام محرك القرص الثابت بالكمبيوتر أو فك تشفير أي قسم (أقسام) تم تشفيره بالفعل في محرك القرص.

١. ابدأ تشغيل **Drive Encryption**. للحصول على مزيد من المعلومات، انظر فتح Drive Encryption في صفحة ٢٦.

٢. ضمن **Drive Status** (حالة القرص)، حدد أو ألغِ تحديد خانة الاختيار المجاورة لكل قسم من أقسام محرك القرص الثابت تريد تشفيره أو فك تشفيره، ثم انقر فوق أو اضغط على **Apply** (تطبيق).

ملاحظة: خلال عملية تشفير القسم أو فك تشفيره، يعرض شريط التقدم النسبة المئوية للقسم المشفر.

ملاحظة: هذه الميزة غير متاحة للأقسام الديناميكية. إذا تم عرض القسم بوصفه متوفرًا، لكن تعذر تشفيره عند تحديده، فهذا قسم ديناميكي. ينتج القسم الديناميكي من تقليص حجم القسم لإنشاء قسم جديد ضمن إدارة القرص.

ويتم عرض تحذير إذا كان أحد الأقسام سيتم تحويله إلى قسم ديناميكي.

إدارة القرص

- **Nickname** (الاسم البديل) — يمكنك إطلاق أسماء على محركات الأقراص أو الأقسام لتسهيل التعرف عليها.
- **Disconnected drives** (محركات الأقراص غير المتصلة) — يمكن من خلال Drive Encryption تتبع الأقراص التي تمت إزالتها من الكمبيوتر. ويتم نقل القرص الذي تتم إزالته من الكمبيوتر تلقائيًا إلى قائمة محركات الأقراص غير المتصلة. فإذا تمت إعادة القرص إلى النظام، فسيظهر من جديد في قائمة محركات الأقراص المتصلة.
- إذا لم تُعد بحاجة إلى تتبع محرك القرص غير المتصل أو إدارته، يمكنك إزالة المحرك غير المتصل من قائمة محركات الأقراص غير المتصلة.
- يظل Drive Encryption في وضع التنشيط حتى يتم إلغاء تحديد خانات الاختيار لجميع محركات الأقراص المتصلة، وإفراغ قائمة محركات الأقراص غير المتصلة.

النسخ الاحتياطي والاسترداد (مهمة المسؤول)

عند تنشيط Drive Encryption، يمكن للمسؤولين استخدام صفحة Encryption Key Backup (النسخ الاحتياطي لمفتاح التشفير) لنسخ مفاتيح التشفير احتياطيًا على وسائط قابلة للإزالة ولتنفيذ عملية الاسترداد.

النسخ الاحتياطي لمفاتيح التشفير

يمكن للمسؤولين نسخ مفتاح تشفير محرك القرص المشفر احتياطيًا على جهاز تخزين قابل للإزالة.

تنبيه: تأكد من الاحتفاظ بجهاز التخزين الذي يحتوي على مفتاح النسخ الاحتياطي في مكان آمن لأنك إذا نسيت كلمة المرور الخاصة بك، أو فقدت البطاقة الذكية أو لم تكن قد سجلت إصبعك، فسيوفر هذا الجهاز لك الطريقة الوحيدة للوصول إلى جهاز الكمبيوتر. كذلك يجب أن يكون مكان التخزين آمنًا لأن جهاز التخزين يسمح بالوصول إلى Windows.

١. ابدأ تشغيل **Drive Encryption**. للحصول على مزيد من المعلومات، انظر فتح Drive Encryption في صفحة ٢٦.

٢. حدد خانة الاختيار الخاصة بأحد محركات الأقراص، ثم انقر فوق أو اضغط على **Backup Key** (مفتاح النسخ الاحتياطي).

٣. ضمن **Create HP Drive Encryption recovery key** (إنشاء مفتاح استرداد HP Drive Encryption)، حدد خيارًا أو أكثر من بين الخيارات التالية:

- **Removable Storage** (وحدة تخزين قابلة للإزالة) — حدد خانة الاختيار، ثم حدد جهاز التخزين الذي سيتم تخزين مفتاح التشفير عليه.
- **SkyDrive** — حدد خانة الاختيار. يجب أن تكون متصلاً بالإنترنت. سجّل الدخول إلى Microsoft SkyDrive، ثم انقر فوق أو اضغط على **Yes** (نعم).

ملاحظة: لاستخدام مفتاح النسخ الاحتياطي لبرنامج HP Drive Encryption الذي خزنته في SkyDrive، يجب تنزيله من SkyDrive إلى جهاز تخزين قابل للإزالة، ثم إدخال جهاز التخزين في هذا الكمبيوتر.

- **TPM** (طُرز معينة فقط) — يسمح لك باسترداد البيانات باستخدام كلمة مرور TPM.

تنبيه: إذا تم مسح TPM أو تعرض الكمبيوتر للتلف، فستفقد إمكانية الوصول إلى النسخة الاحتياطية. إذا تم تحديد هذه الطريقة، يجب تحديد طريقة نسخ احتياطي أخرى كذلك.

٤. انقر فوق أو اضغط على **Backup** (نسخ احتياطي).

فيتم حفظ مفتاح التشفير على جهاز التخزين الذي اخترته.

استرداد إمكانية الوصول إلى كمبيوتر تم تنشيطه باستخدام مفاتيح النسخ الاحتياطي

يمكن للمسؤولين إجراء عملية استرداد باستخدام مفتاح Drive Encryption المنسوخ احتياطيًا على جهاز تخزين قابل للإزالة عند التنشيط أو بتحديد خيار **Backup Key** (مفتاح النسخ الاحتياطي) في Drive Encryption.

١. أدخل جهاز التخزين القابل للإزالة والذي يحتوي على مفتاح النسخ الاحتياطي الخاص بك.

٢. شغّل الكمبيوتر.

٣. عند فتح مربع حوار تسجيل الدخول إلى HP Drive Encryption، انقر فوق أو اضغط على **Recovery** (استرداد).

٤. أدخل مسار الملف الذي يتضمن مفتاح النسخ الاحتياطي أو اسمه، ثم انقر فوق أو اضغط على **Recovery** (استرداد).

٥. عند فتح مربع حوار التأكيد، انقر فوق أو اضغط على **OK** (موافق).

فيتم عرض شاشة تسجيل الدخول إلى Windows.

ملاحظة: إذا تم استخدام مفتاح الاسترداد لتسجيل الدخول في شاشة تسجيل الدخول إلى Drive Encryption، فسيتطلب الأمر بيانات اعتماد إضافية عند تسجيل الدخول إلى Windows للوصول إلى حسابات المستخدمين. يوصى بشدة بإعادة تعيين كلمة المرور بعد تنفيذ أية عملية استرداد.

تنفيذ الاسترداد من خلال HP SpareKey

يتطلب الاسترداد من خلال SpareKey ضمن مرحلة ما قبل تمهيد Drive Encryption الإجابة عن أسئلة الحماية بطريقة صحيحة قبل أن يتاح لك الوصول إلى الكمبيوتر. للحصول على مزيد من المعلومات بشأن إعداد الاسترداد من خلال SpareKey، انظر تعليمات برنامج HP Client Security.

لتنفيذ الاسترداد باستخدام HP SpareKey في حالة نسيان كلمة المرور:

١. شغّل الكمبيوتر.

٢. عند عرض صفحة HP Drive Encryption، انتقل إلى صفحة تسجيل دخول المستخدم.

٣. انقر فوق **SpareKey** (موافق).

ملاحظة: إذا لم يبدأ تشغيل SpareKey في HP Client Security، فلن يكون زر **SpareKey** متوفرًا.

٤. اكتب الإجابات الصحيحة عن الأسئلة المعروضة، ثم انقر فوق أو اضغط على **Logon** (تسجيل الدخول).

فيتم عرض شاشة تسجيل الدخول إلى Windows.

ملاحظة: إذا تم استخدام SpareKey لتسجيل الدخول في شاشة تسجيل الدخول إلى Drive Encryption، فسيتطلب الأمر بيانات اعتماد إضافية عند تسجيل الدخول إلى Windows للوصول إلى حسابات المستخدمين. يوصى بشدة بإعادة تعيين كلمة المرور بعد تنفيذ أية عملية استرداد.

٦ HP File Sanitizer (طُرز محددة فقط)

يسمح لك File Sanitizer بإتلاف الأصول بشكل آمن (على سبيل المثال: كالمعلومات الشخصية أو الملفات أو بيانات المحفوظات أو البيانات المتعلقة بالويب أو عناصر البيانات الأخرى) على محرك القرص الثابت الداخلي للكمبيوتر بأمان وتقليل المساحة الحرة على محرك القرص الثابت للكمبيوتر بصفة دورية.

ولا يمكن استخدام File Sanitizer لتنظيف أنواع محركات الأقراص التالية تمامًا أو تقليل المساحة الحرة عليها:

- محركات الأقراص صلبة الحالة (SSD)، بما في ذلك وحدات تخزين RAID التي يتم توزيعها على جهاز به محرك أقراص صلب الحالة
- محركات الأقراص الخارجية المتصلة عبر واجهة USB أو Firewire أو eSATA

إذا حاولت تنفيذ عملية إتلاف البيانات على محرك أقراص صلب الحالة أو تقليل المساحة الحرة عليه، فسيتم عرض رسالة تحذير ولن يتم تنفيذ العملية.

إتلاف

يختلف الإتلاف عن إجراء الحذف الاعتيادي في أنظمة تشغيل Windows®. فعند إتلاف أحد الأصول باستخدام File Sanitizer، تُكتب بيانات ليس لها معنى في موضع الملفات نفسه، مما يجعل استرجاع الأصل الأصلي مستحيلاً من الناحية الفعلية. بينما قد يترك الإجراء البسيط للحذف في Windows الملف (أو الأصل) سليمًا على محرك القرص الثابت أو في حالة تسمح باستخدام طرق البحث الجنائي لاسترجاعه.

يمكنك تحديد توقيت الإتلاف في المستقبل أو يمكنك تنشيط إتلاف البيانات يدويًا من خلال تحديد أيقونة **File Sanitizer** في الشاشة الرئيسية لتطبيق HP Client Security أو باستخدام أيقونة **File Sanitizer** على سطح مكتب Windows. للحصول على مزيد من المعلومات، راجع تعيين جدول الإتلاف في صفحة ٣٤ أو الإتلاف بالنقر بزر الماوس الأيمن في صفحة ٣٥ أو بدء عملية الإتلاف يدويًا في صفحة ٣٦.

ملاحظة: لا يتم إتلاف الملفات بتنسيق dll. وإزالتها من النظام إلا في حال نقلها إلى سلة المحذوفات.

تقليل المساحة الحرة

لا يزيل حذف أحد الأصول في نظام التشغيل Windows محتويات الأصل المذكور تمامًا من محرك القرص الثابت. بل يحذف نظام التشغيل Windows فقط الإشارة إلى الأصل أو موقعه على محرك القرص الثابت. لكن محتوى الأصل سيظل على محرك القرص الثابت إلى أن تتم كتابة أصل آخر بمعلوماته الجديدة على تلك المساحة نفسها في محرك القرص الثابت.

يسمح لك تقليل المساحة الحرة بكتابة بيانات عشوائية بطريقة آمنة فوق الأصول المحذوفة، مما يحول دون قيام المستخدمين بعرض المحتويات الأصلية للأصل المحذوف.

ملاحظة: لا توفر ميزة تقليل المساحة الحرة أي أمان إضافي للأصول التي تم إتلافها.

يمكن تحديد وقت تقليل المساحة الحرة في المستقبل، أو تنشيط تقليل المساحة الحرة يدويًا للأصول التي تم إتلافها سابقًا من خلال تحديد أيقونة **File Sanitizer** في الشاشة الرئيسية لتطبيق HP Client Security أو باستخدام أيقونة **File Sanitizer** على سطح مكتب Windows. للحصول على مزيد من المعلومات، راجع تعيين جدول لتقليل المساحة الحرة في صفحة ٣٤ أو بدء تقليل المساحة الحرة يدويًا في صفحة ٣٦ أو استخدام أيقونة File Sanitizer في صفحة ٣٥.

فتح File Sanitizer

١. من شاشة Start (ابدأ)، انقر فوق أو اضغط على تطبيق **HP Client Security** (في نظام التشغيل Windows 8).

– أو –

من سطح مكتب Windows، انقر نقرًا مزدوجًا فوق أيقونة **HP Client Security** في منطقة الإعلام بأقصى يمين شريط المهام، أو اضغط عليها ضغطًا مزدوجًا.

٢. ضمن **Data** (البيانات)، انقر فوق أو اضغط على **File Sanitizer**.

– أو –

▲ انقر نقرًا مزدوجًا فوق أيقونة **File Sanitizer** على سطح مكتب Windows أو اضغط عليها ضغطًا مزدوجًا.

– أو –

▲ انقر بزر الماوس الأيمن فوق أيقونة **File Sanitizer** أو اضغط عليها مع الاستمرار على سطح مكتب Windows، ثم حدد **Open File Sanitizer** (فتح File Sanitizer).

إجراءات الإعداد

الإتلاف— يعمل File Sanitizer على حذف أو إتلاف فئات الأصول المحددة بشكل آمن.

١. ضمن **Shredding** (إتلاف)، حدد خانة الاختيار أمام كل نوع من أنواع الملفات ليتم إتلافها، أو ألغِ تحديد خانة الاختيار إذا كنت لا ترغب في إتلاف هذه الملفات.

- **Recycle Bin** (سلة المحذوفات) — لإتلاف جميع العناصر داخل سلة المحذوفات.
- **Temporary system files** (ملفات النظام المؤقتة) — لإتلاف كل الملفات في المجلد المؤقت للنظام. يتم البحث عن متغيرات بيئة التشغيل التالية بالترتيب التالي ويتم اعتبار أول مسار يتم إيجاده مجلد النظام:
  - TMP
  - TEMP
- **Temporary Internet files** (ملفات الإنترنت المؤقتة) — لإتلاف نُسخ صفحات الويب والصور والوسائط التي يتم حفظها من خلال مستعرضات الويب للعرض بشكل أسرع.
- **Cookies** (ملفات تعريف الارتباط) — لإتلاف جميع الملفات التي يتم تخزينها على الكمبيوتر من قِبل مواقع الويب لحفظ التفضيلات، مثل معلومات تسجيل الدخول.

٢. لبدء الإتلاف، انقر فوق أو اضغط على **Shred** (إتلاف).

تقليل المساحة الحرة — لكتابة بيانات عشوائية على المساحة الحرة ومنع استرداد العناصر المحذوفة.

▲ لبدء تقليل المساحة الحرة، انقر فوق أو اضغط على **Bleach** (تقليل المساحة الحرة).

خيارات File Sanitizer — حدد خانة الاختيار لتمكين أحد الخيارات التالية أو ألغِ تحديد خانة الاختيار لتعطيل الخيار:

- **Enable Desktop icon** (تمكين أيقونة سطح المكتب) — لعرض أيقونة File Sanitizer على سطح مكتب Windows.
- **Enable right-click** (تمكين النقر بزر الماوس الأيمن) — يسمح باستخدام النقر بزر الماوس الأيمن فوق أحد الأصول أو الضغط مع الاستمرار عليه، ثم تحديد **HP File Sanitizer – Shred** (HP File Sanitizer – إتلاف).
- **Ask for Windows password before manual shredding** (طلب كلمة مرور Windows قبل الإتلاف اليدوي) — يتطلب المصادقة باستخدام كلمة مرور Windows قبل إتلاف عنصر يدويًا.
- **Shred Cookies and Temporary Internet Files on browser close** (إتلاف ملفات تعريف الارتباط وملفات الإنترنت المؤقتة عند إغلاق المستعرض) — لإتلاف جميع الأصول المحددة والمرتبطة بالويب، مثل محفوظات المستعرض من عناوين URL عند إغلاقك مستعرض الويب.

تعيين جدول الإتلاف

يمكنك تحديد توقيت لتنفيذ عملية الإتلاف فيه تلقائيًا، أو يمكنك كذلك إتلاف الأصول يدويًا في أي وقت. للحصول على مزيد من المعلومات، راجع إجراءات الإعداد في صفحة ٣٣.

١. افتح File Sanitizer، ثم انقر فوق أو اضغط على **Settings** (الإعدادات).

٢. لتحديد توقيت مستقبلي لإتلاف الأصول المحددة فيه، ضمن **Shred Schedule** (جدول الإتلاف)، حدد **Never** (مطلقًا)، أو **Once** (مرة واحدة)، أو **Daily** (يوميًا)، أو **Weekly** (أسبوعيًا)، أو **Monthly** (شهريًا)، ثم حدد اليوم والوقت:

أ. انقر فوق أو اضغط على حقل الساعة أو الدقيقة أو AM/PM (صباحًا/مساءً).

ب. مرر حتى يتم عرض القيمة المطلوبة في المستوى نفسه للحقول الأخرى.

ج. انقر فوق أو اضغط على المساحة البيضاء المحيطة بحقول تعيين الوقت.

د. كرر الخطوات نفسها مع كل حقل حتى تنتهي من تحديد الجدول الصحيح.

٣. الأنواع الأربعة التالية للأصول مدرجة:

- **Recycle Bin** (سلة المحذوفات) — لإتلاف جميع العناصر داخل سلة المحذوفات.
- **Temporary system files** (ملفات النظام المؤقتة) — لإتلاف كل الملفات في المجلد المؤقت للنظام. يتم البحث عن متغيرات بيئة التشغيل التالية بالترتيب التالي ويتم اعتبار أول مسار يتم إيجاده مجلد النظام:
  - TMP
  - TEMP
- **Temporary Internet files** (ملفات الإنترنت المؤقتة) — لإتلاف نُسخ صفحات الويب والصور والوسائط التي يتم حفظها من خلال مستعرضات الويب للعرض بشكل أسرع.
- **Cookies** (ملفات تعريف الارتباط) — لإتلاف جميع الملفات التي يتم تخزينها على الكمبيوتر من قِبل مواقع الويب لحفظ التفضيلات، مثل معلومات تسجيل الدخول.

إذا تم تحديدها، فسيتم إتلاف هذه الأصول في الوقت المحدد بالجدول.

٤. لتحديد أصول إضافية مخصصة لإتلافها:

أ. ضمن **Scheduled Shred List** (قائمة الإتلاف المجدول)، انقر فوق أو اضغط على **Add folder** (إضافة مجلد)، ثم انتقل إلى الملف أو المجلد.

ب. انقر فوق أو اضغط على **Open** (فتح)، ثم انقر فوق أو اضغط على **OK** (موافق).

لإزالة أصل من قائمة الإتلاف المجدول، ألغِ تحديد خانة الاختيار للأصل المقصود.

تعيين جدول لتقليل المساحة الحرة

لا توفر ميزة تقليل المساحة الحرة أي أمان إضافي للأصول التي تم إتلافها.

١. افتح File Sanitizer، ثم انقر فوق أو اضغط على **Settings** (الإعدادات).

٢. لتحديد توقيت مستقبلي لتقليل المساحة الحرة على محرك القرص الثابت، ضمن **Bleach Schedule** (جدول تقليل المساحة الحرة)، حدد **Never** (مطلقًا)، أو **Once** (مرة واحدة)، أو **Daily** (يوميًا)، أو **Weekly** (أسبوعيًا)، أو **Monthly** (شهريًا)، ثم حدد اليوم والوقت.

أ. انقر فوق أو اضغط على حقل الساعة أو الدقيقة أو AM/PM (صباحًا/مساءً).

ب. مرر حتى يتم عرض الوقت المطلوب في المستوى نفسه للحقول الأخرى.

ج. انقر فوق أو اضغط على المساحة البيضاء المحيطة بحقول تعيين الوقت.

د. كرر الخطوات نفسها حتى تنتهي من تحديد الجدول الصحيح.

ملاحظة: قد تستغرق عملية تقليل المساحة الحرة فترة طويلة من الوقت. تأكد من اتصال الكمبيوتر بمصدر طاقة للتيار المتناوب. على الرغم من تنفيذ عملية تقليل المساحة الحرة في الخلفية، لكن الاستخدام الزائد للمعالج قد يؤثر على أداء الكمبيوتر. فيمكن تنفيذ عملية تقليل المساحة الحرة بعد ساعات أو عند عدم استخدام الكمبيوتر.

حماية الملفات من الإتلاف

لحماية الملفات أو المجلدات من الإتلاف:

١. افتح File Sanitizer، ثم انقر فوق أو اضغط على **Settings** (الإعدادات).

٢. ضمن **Never Shred List** (قائمة عدم الإتلاف مطلقًا)، انقر فوق أو اضغط على **Add folder** (إضافة مجلد)، ثم انتقل إلى الملف أو المجلد.

٣. انقر فوق أو اضغط على **Open** (فتح)، ثم انقر فوق أو اضغط على **OK** (موافق).

ملاحظة: تتوفر الحماية للملفات في هذه القائمة طالما بقيت داخل القائمة.

لإزالة أصل من قائمة الاستثناءات، ألغِ تحديد خانة الاختيار الخاصة بذلك الأصل.

المهام العامة

استخدم File Sanitizer لتنفيذ المهام التالية:

- **استخدم أيقونة File Sanitizer لبدء الإتلاف** — اسحب الملفات إلى أيقونة **File Sanitizer** على سطح مكتب Windows. للاطلاع على التفاصيل، راجع استخدام أيقونة File Sanitizer في صفحة ٣٥.
- **الإتلاف اليدوي لأصل محدد أو لجميع الأصول المحددة** — لإتلاف العناصر في أي وقت دون انتظار وقت الإتلاف المحدد بالجدول. للاطلاع على التفاصيل، راجع الإتلاف بالنقر بزر الماوس الأيمن في صفحة ٣٥ أو بدء عملية الإتلاف يدويًا في صفحة ٣٦.
- **التنشيط اليدوي لتقليل المساحة الحرة** — لتنشيط تقليل المساحة الحرة في أي وقت. للاطلاع على التفاصيل، راجع بدء تقليل المساحة الحرة يدويًا في صفحة ٣٦.
- **عرض ملفات السجل** — لعرض ملفات سجل الإتلاف وتقليل المساحة الحرة والتي تحتوي على أية أخطاء أو أعطال من آخر عملية إتلاف أو تقليل للمساحة الحرة. للاطلاع على التفاصيل، راجع عرض ملفات السجل في صفحة ٣٦.

ملاحظة: قد تستغرق عملية الإتلاف أو تقليل المساحة الحرة فترة طويلة من الوقت. على الرغم من تنفيذ عملية الإتلاف وتقليل المساحة الحرة في الخلفية، لكن الاستخدام الزائد للمعالج قد يؤثر على أداء الكمبيوتر.

استخدام أيقونة File Sanitizer

تنبيه: لا يمكن استرداد الأصول التي تم إتلافها. فكر بعناية في العناصر التي تحددها من أجل الإتلاف اليدوي.

عندما تبدأ عملية إتلاف يدويًا، يتم إتلاف قائمة الإتلاف القياسية في طريقة عرض File Sanitizer (انظر إجراءات الإعداد في صفحة ٣٣).

يمكنك بدء عملية الإتلاف يدويًا بإحدى الطرق التالية:

١. افتح File Sanitizer، (انظر فتح File Sanitizer في صفحة ٣٣)، ثم انقر فوق أو اضغط على **Shred** (إتلاف).

٢. عند فتح مربع حوار التأكيد، تأكد من تحديد الأصول التي تريد إتلافها، ثم انقر فوق أو اضغط على **OK** (موافق).

– أو –

١. انقر بزر الماوس الأيمن فوق أيقونة **File Sanitizer** أو اضغط عليها مع الاستمرار على سطح مكتب Windows، ثم انقر فوق أو اضغط على **Shred Now** (إتلاف الآن).

٢. عند فتح مربع حوار التأكيد، تأكد من تحديد الأصول التي تريد إتلافها، ثم انقر فوق أو اضغط على **Shred** (إتلاف).

الإتلاف بالنقر بزر الماوس الأيمن

تنبيه: لا يمكن استرداد الأصول التي تم إتلافها. فكر بعناية في العناصر التي تحددها من أجل الإتلاف اليدوي.

إذا تم تحديد خيار **Enable right-click shredding** (تمكين الإتلاف بالنقر على زر الماوس الأيمن) في طريقة عرض File Sanitizer، فبإمكانك إتلاف أحد الأصول على النحو التالي:

١. انتقل إلى المستند أو المجلد الذي تريد إتلافه.

٢. انقر بزر الماوس الأيمن فوق الملف أو المجلد أو اضغط عليه مع الاستمرار، ثم حدد **HP File Sanitizer – Shred** (HP File Sanitizer – إتلاف).

بدء عملية الإتلاف يدويًا

⚠ **تنبيه:** لا يمكن استرداد الأصول التي تم إتلافها. فكر بعناية في العناصر التي تحددها من أجل الإتلاف اليدوي.

عندما تبدأ عملية إتلاف يدويًا، يتم إتلاف قائمة الإتلاف القياسية في طريقة عرض File Sanitizer (انظر إجراءات الإعداد في صفحة ٣٣).

يمكنك بدء عملية الإتلاف يدويًا بإحدى الطرق التالية:

١. افتح File Sanitizer، (انظر فتح File Sanitizer في صفحة ٣٣)، ثم انقر فوق أو اضغط على **Shred** (إتلاف).

٢. عند فتح مربع حوار التأكيد، تأكد من تحديد الأصول التي تريد إتلافها، ثم انقر فوق أو اضغط على **OK** (موافق).

– أو –

١. انقر بزر الماوس الأيمن فوق أيقونة **File Sanitizer** أو اضغط عليها مع الاستمرار على سطح مكتب Windows، ثم انقر فوق أو اضغط على **Shred Now** (إتلاف الآن).

٢. عند فتح مربع حوار التأكيد، تأكد من تحديد الأصول التي تريد إتلافها، ثم انقر فوق أو اضغط على **Shred** (إتلاف).

بدء تقليل المساحة الحرة يدويًا

عندما تبدأ عملية تقليل المساحة الحرة يدويًا، يتم تقليل المساحة الحرة للمحتوى في قائمة الإتلاف القياسية في طريقة عرض File Sanitizer (انظر إجراءات الإعداد في صفحة ٣٣).

يمكنك بدء عملية تقليل المساحة الحرة يدويًا بإحدى الطرق التالية:

١. افتح File Sanitizer، (انظر فتح File Sanitizer في صفحة ٣٣)، ثم انقر فوق أو اضغط على **Bleach** (تقليل المساحة الحرة).

٢. عند فتح مربع حوار التأكيد، انقر فوق أو اضغط على **OK** (موافق).

– أو –

١. انقر بزر الماوس الأيمن فوق أيقونة **File Sanitizer** أو اضغط عليها مع الاستمرار على سطح مكتب Windows، ثم انقر فوق أو اضغط على **Bleach Now** (تقليل المساحة الحرة الآن).

٢. عند فتح مربع حوار التأكيد، انقر فوق أو اضغط على **Bleach** (تقليل المساحة الحرة).

عرض ملفات السجل

في كل مرة يتم فيها تنفيذ عملية الإتلاف أو تقليل المساحة الحرة، يتم إنشاء ملفات سجل لأية أخطاء أو أعطال. ويتم تحديث ملفات السجل دائمًا وفقًا لآخر عملية إتلاف أو تقليل للمساحة الحرة.

ملاحظة: لا تظهر الملفات التي يتم بنجاح إتلافها أو تقليل المساحة الحرة الخاصة بها في ملفات السجل.

يتم إنشاء ملف سجل واحد لعمليات الإتلاف، وإنشاء ملف سجل آخر لعمليات تقليل المساحة الحرة. ويوجد كلا ملفي السجل على محرك القرص الثابت في المجلدين التاليين:

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

بالنسبة لأنظمة ٦٤ بت، توجد ملفات السجل على محرك القرص الثابت في المجلدين التاليين:

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

٧ HP Device Access Manager (طُرز محددة فقط)

يتحكم برنامج HP Device Access Manager في إمكانية الوصول إلى البيانات من خلال تعطيل أجهزة نقل البيانات.

ملاحظة: لا يتحكم Device Access Manager في بعض أجهزة الإدخال/الواجهة البشرية، مثل الماوس ولوحة المفاتيح ولوحة اللمس وقارئ بصمات الأصابع. للحصول على مزيد من المعلومات، انظر فئات الأجهزة غير المدارة في صفحة ٤١.

يستخدم مسؤولو نظام تشغيل Windows® برنامج HP Device Access Manager للتحكم في إمكانية الوصول إلى الأجهزة الموجودة على نظام ما وللحماية من الوصول غير المصرح به:

- يتم إنشاء ملفات تعريف الأجهزة لكل مستخدم بهدف تحديد الأجهزة المسموح لهم بالوصول إليها أو تلك التي رُفض الترخيص لهم بالوصول إليها.
- تتيح المصادقة في الوقت المناسب (JITA) للمستخدمين المحددين مسبقًا مصادقة أنفسهم للوصول إلى الأجهزة التي لا يحق لهم الوصول إليها إلا دون مصادقة.
- يمكن استبعاد المسؤولين والمستخدمين الموثوق بهم من القيود، التي فرضها Device Access Manager، المفروضة على الوصول للأجهزة وذلك عن طريق إضافتهم إلى مجموعة المسؤولين عن الأجهزة. وتتم إدارة العضوية في هذه المجموعة باستخدام الإعدادات المتقدمة.
- يمكن الموافقة على إمكانية الوصول للأجهزة أو رفضها بناء على عضوية مجموعة مستخدمين أو لمستخدمين أفراد.
- بالنسبة إلى فئات الأجهزة مثل محركات أقراص CD-ROM ومحركات أقراص DVD، يمكن السماح بحق الوصول للقراءة والكتابة أو رفض الوصول بشكل منفصل.

يتم تكوين HP Device Access Manager بصورة تلقائية بالإعدادات التالية أثناء إكمال معالج إعداد برنامج HP Client Security:

- تكون الوسائط القابلة للإزالة الخاصة بالمصادقة في الوقت المناسب ممكّنة للمسؤولين والمستخدمين.
- تسمح السياسة الخاصة بالجهاز بالوصول الكامل لأجهزة أخرى.

فتح Device Access Manager

١. من شاشة Start (ابدأ)، انقر فوق أو اضغط على تطبيق **HP Client Security** (في نظام التشغيل Windows 8).

– أو –

من سطح مكتب Windows، انقر نقرًا مزدوجًا فوق أيقونة **HP Client Security** في منطقة الإعلام بأقصى يمين شريط المهام، أو اضغط عليها ضغطًا مزدوجًا.

٢. ضمن **Device** (الجهاز)، انقر فوق أو اضغط على **Device Permissions** (أذونات الأجهزة).

- يمكن للمستخدمين القياسيين عرض بيانات وصول جهازهم الحالي (انظر طريقة عرض المستخدم في صفحة ٣٩).
- يمكن للمسؤولين عرض بيانات وصول الجهاز المكوّن حاليًا للكمبيوتر وإجراء تغييرات عليه من خلال النقر فوق أو الضغط على **Change** (تغيير)، ثم إدخال كلمة مرور المسؤول (انظر طريقة عرض النظام في صفحة ٣٩).

طريقة عرض المستخدم

عند تحديد **Device Permissions** (أذونات الأجهزة)، يتم عرض طريقة عرض المستخدم. تبعًا للسياسة، يمكن للمسؤولين وللمستخدمين القياسيين مشاهدة بيانات الوصول الخاص بهم لفئات الأجهزة أو الأجهزة المفردة على هذا الكمبيوتر.

- **Current user** (المستخدم الحالي) — يتم عرض اسم المستخدم المسجل دخوله حاليًا.
- **Device Class** (فئة الجهاز) — يتم عرض أنواع الأجهزة.
- **Access** (الوصول) — يتم عرض بيانات الوصول المكوّن حاليًا لأنواع الأجهزة أو لأجهزة معينة.
- **Duration** (المدة) — يتم عرض الحد الزمني الخاص بوصولك لمحركات أقراص CD/DVD-ROM أو محركات الأقراص القابلة للإزالة.
- **Settings** (الإعدادات) — يمكن للمسؤولين تغيير محركات الأقراص التي يتم التحكم في الوصول إليها من خلال Device Access Manager.

طريقة عرض النظام

من شاشة طريقة عرض النظام، يمكن للمسؤولين السماح بالوصول للأجهزة الموجودة على هذا الكمبيوتر أو رفض هذا الوصول لمجموعة مستخدمين أو لمجموعة مسؤولين.

▲ يمكن للمسؤولين الوصول إلى طريقة عرض النظام من خلال النقر فوق أو الضغط على **Change** (تغيير) وإدخال كلمة مرور المسؤول، ثم الاختيار من بين الخيارات التالية:

- **Device Access Manager** — لتشغيل HP Device Access Manager مع ميزة المصادقة في الوقت المناسب أو إيقاف تشغيله، انقر فوق أو اضغط على **On** (تشغيل) أو **Off** (إيقاف التشغيل).
- **Users and groups on this PC** (المستخدمون والمجموعات على هذا الكمبيوتر) — لعرض مجموعة المستخدمين أو مجموعة المسؤولين المسموح بوصولهم لفئات الأجهزة المحددة أو المرفوض وصولهم إليها.
- **Device Class** (فئة الجهاز) — لعرض فئات الأجهزة والأجهزة التي يتم تركيبها على النظام أو الأجهزة التي ربما تم تركيبها من قبل على النظام. لتوسيع القائمة، انقر فوق الأيقونة **+**. يتم عرض جميع الأجهزة المتصلة بالكمبيوتر، وتوسيع مجموعة المسؤولين والمستخدمين لعرض عضوية كل منهم. لتحديث قائمة الأجهزة، انقر فوق أيقونة (تحديث) ذات السهم الدائري.
  - يتم عادة تطبيق الحماية على فئة الجهاز. في حالة تعيين إمكانية الوصول على **Allow** (سماح)، فسيكون بإمكان المستخدم المحدد أو المجموعة المحددة الوصول إلى أي جهاز في فئة الجهاز تلك.
  - ويمكن أيضًا تطبيق الحماية على أجهزة معينة.
  - قم بتكوين المصادقة في الوقت المناسب، بما يسمح للمستخدمين المحددين بالوصول إلى محركات أقراص DVD/CD-ROM أو محركات الأقراص القابلة للإزالة من خلال مصادقة أنفسهم. للحصول على مزيد من المعلومات، انظر تكوين المصادقة في الوقت المناسب في صفحة ٤٠.
  - اسمح بالوصول إلى فئات أجهزة أخرى، مثل الوسائط القابلة للإزالة (مثل محركات USB المحمولة)، والمنافذ التسلسلية والمتوازية، والأجهزة التي تعمل بتقنية Bluetooth®، وأجهزة المودم، وأجهزة PCMCIA/ExpressCard، وأجهزة ١٣٩٤، وقارئ بصمة الإصبع، وقارئ البطاقات الذكية أو رفض الوصول إليها. في حالة رفض إمكانية الوصول إلى قارئ بصمة الإصبع وقارئ البطاقات الذكية، فيمكن استخدامهما كبيانات اعتماد للمصادقة، ولكن لا يمكن استخدامهما عند مستوى سياسة جلسة العمل.

ملاحظة: في حالة استخدام الأجهزة التي تعمل بتقنية Bluetooth كبيانات اعتماد للمصادقة، فلا ينبغي تقييد إمكانية وصول الجهاز الذي يعمل بتقنية Bluetooth في سياسة Device Access Manager.

  - عند تحديد إعداد في مستوى فئة جهاز أو مجموعة، ومطالبتك بتحديد ما إذا كان سيتم تطبيق الإعداد على الكائنات التابعة أم لا:

    Yes (نعم) — سيمتد الإعداد إلى الكائنات التابعة.

    No (لا) — لن يمتد الإعداد إلى الكائنات التابعة.
  - ربما يتم التحكم بشكل أكبر في بعض فئات الأجهزة، مثل أقراص DVD وأقراص CD-ROM، من خلال السماح بالوصول بشكل منفصل إلى عمليات القراءة والكتابة أو رفض ذلك الوصول.

ملاحظة: لا يمكن إضافة مجموعة المسؤولين إلى قائمة المستخدمين.

- **Access** (الوصول) — انقر فوق أو اضغط على سهم لأسفل، ثم حدد أحد أنواع الوصول التالية للسماح بالوصول أو رفضه:
  - **Allow – Full Access** (سماح - وصول كامل)
  - **Allow – Read Only** (سماح - قراءة فقط)
  - **Allow – JITA Required** (سماح - تلزم المصادقة في الوقت المناسب) — للحصول على مزيد من المعلومات، انظر تكوين المصادقة في الوقت المناسب في صفحة ٤٠.

    في حالة تحديد هذا النوع من الوصول، ضمن **Duration** (المدة)، انقر فوق أو اضغط على سهم لأسفل لتحديد حد زمني.
  - **Deny** (رفض)
- **Duration** (المدة) — انقر فوق أو اضغط على سهم لأسفل لتحديد حد زمني للوصول إلى محركات أقراص CD/DVD-ROM أو إلى محركات الأقراص القابلة للإزالة (انظر تكوين المصادقة في الوقت المناسب في صفحة ٤٠).

تكوين المصادقة في الوقت المناسب

يسمح تكوين المصادقة في الوقت المناسب للمسؤول بالاطلاع على وتعديل قوائم المستخدمين والمجموعات المسموح لهم بالوصول إلى الأجهزة باستخدام المصادقة في الوقت المناسب.

سيكون بمقدور المستخدمين الممكن لديهم ميزة المصادقة في الوقت المناسب الوصول إلى بعض الأجهزة التي تم تقييد السياسات المنشأة لها في طريقة عرض **Device Class Configuration** (تكوين فئة الجهاز).

يمكن ترخيص مدة المصادقة في الوقت المناسب لعدد محدد من الدقائق أو بجعلها غير محدودة. وسيكون للمستخدمين غير المحدودين إمكانية الوصول إلى الجهاز بدءًا من الوقت الذي تمت مصادقتهم فيه وحتى تسجيل خروجهم من النظام.

إذا مُنح المستخدم مدة محددة للمصادقة في الوقت المناسب، فسيُطلب من المستخدم تحديد ما إذا كان يريد مد الفترة الزمنية لحق الوصول أم لا وذلك قبل دقيقة واحدة من انقضاء مدة المصادقة في الوقت المناسب. بمجرد تسجيل خروج المستخدم من النظام أو قيام مستخدم آخر بتسجيل دخوله، تنقضي مدة المصادقة في الوقت المناسب. في المرة التالية التي يسجل فيها المستخدم دخوله ويحاول الوصول إلى الجهاز الممكن فيه ميزة المصادقة في الوقت المناسب، يتم عرض رسالة تطلب إدخال بيانات الاعتماد.

تتوفر ميزة المصادقة في الوقت المناسب لفئات الأجهزة التالية:

- محركات أقراص DVD/CD-ROM
- محركات الأقراص القابلة للإزالة

إنشاء سياسة المصادقة في الوقت المناسب لمستخدم أو لمجموعة

بمقدور المسؤولين السماح للمستخدمين أو للمجموعات بالوصول إلى الأجهزة باستخدام المصادقة في الوقت المناسب.

١. ابدأ تشغيل **Device Access Manager**، ثم انقر فوق أو اضغط على **Change** (تغيير).

٢. حدد المستخدم أو المجموعة، ثم ضمن **Access** (الوصول) لأي من **Removable Disk drives** (محركات الأقراص القابلة للإزالة) أو **DVD/CD-ROM drives** (محركات أقراص DVD/CD-ROM)، انقر فوق أو اضغط على سهم لأسفل، ثم حدد **Allow – JITA Required** (سماح - تلزم المصادقة في الوقت المناسب).

٣. ضمن **Duration** (المدة)، انقر فوق أو اضغط على سهم لأسفل لتحديد فترة زمنية لوصول المصادقة في الوقت المناسب.

يجب على المستخدم تسجيل الخروج، ثم تسجيل الدخول مرة أخرى لتطبيق إعداد المصادقة في الوقت المناسب الجديد.

تعطيل سياسة المصادقة في الوقت المناسب لمستخدم أو لمجموعة

يمكن للمسؤولين تعطيل وصول مستخدم أو مجموعة إلى أجهزة باستخدام المصادقة في الوقت المناسب.

١. ابدأ تشغيل **Device Access Manager**، ثم انقر فوق أو اضغط على **Change** (تغيير).

٢. حدد المستخدم أو المجموعة، ثم ضمن **Access** (الوصول) لأي من **Removable Disk drives** (محركات الأقراص القابلة للإزالة) أو **DVD/CD-ROM drives** (محركات أقراص DVD/CD-ROM)، انقر فوق أو اضغط على سهم لأسفل، ثم حدد **Deny** (رفض).

عند قيام المستخدم بتسجيل دخوله ومحاولته الوصول إلى الجهاز، فسيتم رفض الوصول.

الإعدادات

تسمح طريقة عرض **Settings** (الإعدادات) للمسؤولين بعرض المحركات التي يتم التحكم في الوصول إليها من خلال Device Access Manager وتغيير هذه المحركات.

ملاحظة: يجب تمكين Device Access Manager عند تكوين قائمة أحرف محركات الأقراص (انظر طريقة عرض النظام في صفحة ٣٩).

فئات الأجهزة غير المدارة

لا يدير HP Device Access Manager فئات الأجهزة التالية:

- أجهزة الإدخال/الإخراج
  - أقراص CD-ROM
  - محركات الأقراص
  - جهاز التحكم بالأقراص المرنة (FDC)
  - جهاز التحكم بالأقراص الثابتة (HDC)
  - فئة جهاز الواجهة البشرية (HID)
  - أجهزة الواجهة البشرية التي تعمل بالأشعة تحت الحمراء
  - أجهزة الماوس
  - الأجهزة التسلسلية متعددة المنافذ
  - لوحة المفاتيح
  - الطابعات التي تعتمد التوصيل والتشغيل (PnP)
  - الطابعة
  - ترقية الطابعة
- الطاقة
  - دعم إدارة الطاقة المتقدمة (APM)
  - البطارية
- أجهزة متنوعة
  - الكمبيوتر
  - أداة فك الترميز
  - الشاشة
  - محرك أقراص عرض Intel® الموحد
  - Legacard
  - برنامج تشغيل الوسائط
  - الجهاز المغير للوسائط
  - تقنية الذاكرة
  - الشاشة

- الأجهزة متعددة الوظائف
- عميل الشبكة
- خدمة الشبكة
- Net trans
- المعالج
- محول SCSI
- مسرع الحماية
- أجهزة الحماية
- النظام
- الأجهزة غير المعروفة
- وحدة التخزين
- لقطة وحدة التخزين

٨ HP Trust Circles

إن HP Trust Circles هو تطبيق حماية للملفات والمستندات، والذي يجمع بين تشفير ملفات المجلدات وإمكانية المشاركة المناسبة لمستندات بين دوائر موثوق فيها. ويشفر هذا التطبيق الملفات الموجودة في مجلدات خاصة يحددها المستخدم، بما يوفر لها حماية داخل دائرة ثقة. وبمجرد حماية الملفات، فإنه لا يمكن استخدامها ومشاركتها إلا بين الأعضاء في دائرة الثقة. في حالة استلام أحد الأشخاص غير الأعضاء لملف محمي، يظل الملف مشفرًا ولا يمكن لهذا الشخص غير العضو الوصول إلى المحتويات.

فتح Trust Circles

١. في شاشة ابدأ، انقر فوق أو اضغط على تطبيق **HP Client Security**.

– أو –

من سطح مكتب Windows، انقر نقرًا مزدوجًا فوق أيقونة **HP Client Security** في منطقة الإعلام بأقصى يمين شريط المهام.

٢. ضمن **Data** (البيانات)، انقر فوق أو اضغط على **Trust Circles**.

بدء التشغيل

توجد طريقتان لإرسال دعوات عبر البريد الإلكتروني والرد عليها:

- **استخدام Microsoft® Outlook** — يؤدي استخدام Trust Circles من خلال Microsoft Outlook إلى المعالجة التلقائية لأية دعوات واستجابات Trust Circle من مستخدمي Trust Circle الآخرين.
- **استخدام Gmail أو Yahoo أو Outlook.com أو خدمات البريد الإلكتروني الأخرى (SMTP)** — عند إدخال اسمك وعنوان بريدك الإلكتروني وكلمة مرورك، يستخدم تطبيق Trust Circles خدمة بريدك الإلكتروني لإرسال دعوات عبر البريد الإلكتروني إلى الأعضاء المحددين للانضمام إلى دائرة الثقة الخاصة بك.

لإعداد ملف التعريف الرئيسي الخاص بك:

١. أدخل اسمك وعنوان بريدك الإلكتروني، ثم انقر فوق أو اضغط على **Next** (التالي).

يكون الاسم مرئيًا لأي أعضاء مدعوّين للانضمام إلى دائرة الثقة الخاصة بك. يتم استخدام عنوان البريد الإلكتروني لإرسال الدعوات أو تلقيها أو الرد عليها.

٢. أدخل كلمة المرور الخاصة بحساب البريد الإلكتروني، ثم انقر فوق أو اضغط على **Next** (التالي).

يتم إرسال رسالة بريد إلكتروني اختباري للتأكد من دقة إعدادات البريد الإلكتروني.

ملاحظة: يجب أن يكون الكمبيوتر متصلاً بشبكة.

٣. في حقل **Trust Circle Name** (اسم دائرة الثقة)، وأدخل اسمًا لدائرة الثقة، ثم انقر فوق أو اضغط على **Next** (التالي).

٤. أضف الأعضاء والمجلدات، ثم انقر فوق أو اضغط على **Next** (التالي). يتم إنشاء دائرة الثقة التي تحتوي على أي مجلدات تم تحديدها ويتم إرسال دعوات عبر البريد الإلكتروني إلى أي أعضاء تم تحديدهم. في حالة تعذر إرسال دعوة لأي سبب من الأسباب، يتم عرض إشعار. يمكن دعوة الأعضاء مرة أخرى في أي وقت من طريقة عرض Trust Circle بالنقر فوق **Your Trust Circles** (دوائر الثقة الخاصة بك)، ثم النقر المزدوج فوق أو الضغط مرتين على دائرة الثقة. للحصول على مزيد من المعلومات، انظر Trust Circles في صفحة ٤٤.

Trust Circles

يمكنك إنشاء دائرة ثقة أثناء الإعداد الأولي بعد إدخال عنوان بريدك الإلكتروني، أو في طريقة عرض Trust Circle:

▲ من طريقة عرض Trust Circle، انقر فوق أو اضغط على **Create Trust Circle** (إنشاء دائرة ثقة)، ثم أدخل اسمًا لدائرة الثقة.

- لإضافة أعضاء إلى دائرة الثقة، انقر فوق أو اضغط على أيقونة **M+** بجوار **Members** (الأعضاء)، ثم اتبع الإرشادات الظاهرة على الشاشة.
- لإضافة مجلدات إلى دائرة الثقة، انقر فوق أو اضغط على أيقونة **M+** بجوار **Folders** (المجلدات)، ثم اتبع الإرشادات الظاهرة على الشاشة.

إضافة مجلدات إلى دائرة ثقة

إضافة مجلدات إلى دائرة ثقة جديدة:

- أثناء إنشاء دائرة ثقة، يمكنك إضافة مجلدات بالنقر فوق أو الضغط على أيقونة **+** بجوار **Folders** (المجلدات)، ثم اتباع الإرشادات الظاهرة على الشاشة.

– أو –

- في مستكشف Windows، انقر بزر الماوس الأيمن فوق أو اضغط مع الاستمرار على أحد المجلدات الذي لا يعد حاليًا جزءًا من دائرة ثقة، وحدد **Trust Circle** (دائرة ثقة)، ثم حدد **Create Trust Circle from Folder** (إنشاء دائرة ثقة من المجلد).

تلميح: يمكنك تحديد مجلد واحد أو أكثر.

إضافة مجلدات إلى دائرة ثقة موجودة:

- من طريقة عرض Trust Circle (دائرة الثقة)، انقر فوق **Your Trust Circles** (دوائر الثقة الخاصة بك)، وانقر نقرًا مزدوجًا فوق أو اضغط مرتين على دائرة الثقة الموجودة لعرض المجلدات الحالية، وانقر فوق أو اضغط على أيقونة **+** بجوار **Folders** (المجلدات)، ثم اتبع الإرشادات الظاهرة على الشاشة.

– أو –

- في مستكشف Windows، انقر بزر الماوس الأيمن فوق أو اضغط مع الاستمرار على أحد المجلدات الذي لا يعد حاليًا جزءًا من دائرة ثقة، وحدد **Trust Circle** (دائرة ثقة)، ثم حدد **Add to existing Trust Circle from Folder** (إضافة إلى دائرة ثقة موجودة من مجلد).

تلميح: يمكنك تحديد مجلد واحد أو أكثر.

بمجرد إضافة مجلد ما إلى دائرة ثقة، يشفّر Trust Circles هذا المجلد ومحتوياته بصورة تلقائية. بعدها يتم عرض إشعار بمجرد تشفير جميع الملفات. بالإضافة إلى ذلك، يتم عرض رمز قفل أخضر على جميع رموز المجلدات المشفرة ورموز الملفات داخل المجلدات للدلالة على أنها محمية بشكل كامل.

إضافة أعضاء إلى دائرة ثقة

يلزم القيام بثلاث خطوات لإضافة أعضاء إلى دائرة ثقة:

١. **الدعوة** — أولاً، يدعو مالك دائرة الثقة العضو (الأعضاء). ويمكن إرسال دعوة عبر البريد الإلكتروني إلى عدة مستخدمين أو إلى مجموعات/قوائم توزيع.

٢. **القبول** — يتلقى المدعو الدعوة ويقرر ما إذا كان سيقبلها أم يرفضها. في حالة قبول المدعو الدعوة، يتم إرسال استجابة عبر البريد الإلكتروني للداعي. في حالة إرسال الدعوة إلى مجموعة، يتلقى كل عضو دعوة ويقرر ما إذا كان سيقبلها أم يرفضها.

٣. **التسجيل** — تكون أمام الداعي فرصة أخيرة لتحديد ما إذا كان سيضيف العضو إلى دائرة الثقة أم لا. إذا قرر الداعي تسجيل العضو، فسيتم إرسال بريد إلكتروني إلى المدعو بما يمثل إقرارًا بوصول الاستجابة. يمكن لكل من الداعي والمدعو التحقق اختياريًا من أمان عملية الدعوة. يتم عرض رمز تحقق للمدعو، وهو الرمز الذي تجب قراءته للداعي عبر الهاتف. وبمجرد التحقق من الرمز، يمكن للداعي إرسال البريد الإلكتروني الخاص بالتسجيل النهائي.

إضافة أعضاء إلى دائرة ثقة جديدة:

▲ أثناء إنشاء دائرة ثقة، يمكنك إضافة أعضاء بالنقر فوق أو الضغط على أيقونة **+** بجوار **Members** (الأعضاء)، ثم اتباع الإرشادات الظاهرة على الشاشة.

- في حالة استخدام برنامج Outlook، حدد جهات الاتصال من دفتر عناوين Outlook، ثم انقر فوق **OK** (موافق).
- في حالة استخدام خدمة بريد إلكتروني أخرى، فعليك إما بإضافة عناوين البريد الإلكتروني الجديدة يدويًا إلى Trust Circle، أو يمكنك جلبها من عنوان البريد الإلكتروني المسجل في Trust Circle.

إضافة أعضاء إلى دائرة ثقة موجودة:

▲ من طريقة عرض Trust Circle (دائرة الثقة)، انقر فوق **Your Trust Circles** (دوائر الثقة الخاصة بك)، وانقر نقرًا مزدوجًا فوق أو اضغط مرتين على دائرة الثقة الموجودة لعرض الأعضاء الحاليين، وانقر فوق أو اضغط على أيقونة **+** بجوار **Members** (الأعضاء)، ثم اتبع الإرشادات الظاهرة على الشاشة.

- في حالة استخدام برنامج Outlook، حدد جهات الاتصال من دفتر عناوين Outlook، ثم انقر فوق **OK** (موافق).
- في حالة استخدام خدمة بريد إلكتروني أخرى، فعليك إما بإضافة عناوين البريد الإلكتروني الجديدة يدويًا إلى Trust Circle، أو يمكنك جلبها من عنوان البريد الإلكتروني المسجل في Trust Circle.

إضافة ملفات إلى دائرة ثقة

يمكنك إضافة ملفات إلى دائرة ثقة بإحدى الطرق التالية:

- نسخ الملف أو نقله إلى داخل أحد مجلدات دائرة ثقة موجودة.

– أو –

- في مستكشف Windows، انقر بزر الماوس الأيمن فوق أو اضغط مع الاستمرار على أحد الملفات غير المشفرة حاليًا، وحدد **Trust Circle** (دائرة ثقة)، ثم حدد **Encrypt** (تشفير). ستتم مطالبتك بتحديد دائرة الثقة التي ينبغي إضافة الملف إليها.

تلميح: يمكنك تحديد ملف واحد أو أكثر.

المجلدات المشفرة

يمكن لأي عضو في دائرة ثقة الاطلاع على الملفات التي تنتمي إلى تلك الدائرة وتحريرها.

ملاحظة: لا يجري Trust Circle Manager/Reader مزامنة للملفات بين الأعضاء.

تجب مشاركة الملفات باستخدام الوسائل الموجودة، مثل البريد الإلكتروني أو ftp أو موفري مساحة تخزين مجموعة النظراء. تتم على الفور حماية الملفات المنسوخة إلى مجلد بدائرة ثقة أو منقولة إليه أو منشأة داخله.

إزالة مجلدات من دائرة ثقة

تؤدي إزالة مجلد من دائرة ثقة إلى فك تشفير المجلد وجميع محتوياته وإزالة حمايتها.

- من طريقة عرض Trust Circle (دائرة الثقة)، انقر فوق أو اضغط على **Your Trust Circles** (دوائر الثقة الخاصة بك)، وانقر نقرًا مزدوجًا فوق أو اضغط مرتين على دائرة الثقة الموجودة لعرض المجلدات الحالية، ثم انقر فوق أو اضغط على أيقونة **سلة المهملات** بجوار ذلك المجلد.

– أو –

- في مستكشف Windows، انقر بزر الماوس الأيمن فوق أو اضغط مع الاستمرار على أحد المجلدات الذي يعد حاليًا جزءًا من دائرة ثقة، وحدد **Trust Circle** (دائرة ثقة)، ثم حدد **Remove from trust circle** (إزالة من دائرة الثقة).

تلميح: يمكنك تحديد مجلد واحد أو أكثر.

إزالة ملف من دائرة ثقة

لإزالة ملف من دائرة ثقة، في مستكشف Windows، انقر بزر الماوس الأيمن فوق أو اضغط مع الاستمرار على ملف غير مشفر حاليًا، وحدد **Trust Circle** (دائرة ثقة)، ثم حدد **Decrypt File** (فك تشفير الملف).

إزالة أعضاء من دائرة ثقة

لا يمكن إزالة أي عضو مسجل بشكل كامل من دائرة ثقة. والبديل هو إنشاء دائرة ثقة جديدة تضم جميع الأعضاء الآخرين ونقل جميع الملفات والمجلدات إلى دائرة الثقة الجديدة، ثم حذف دائرة الثقة القديمة. وسيضمن هذا الإجراء أن أي ملفات جديدة يتلقاها العضو ستكون غير متاحة للوصول إليها، لكن سيظل بإمكان عضو الدائرة القديمة الوصول إلى أية ملفات تمت مشاركتها سابقًا.

إذا كان هناك عضو غير مسجل بشكل كامل (في حالة دعوة العضو للانضمام إلى دائرة الثقة أو عدم قبول العضو الدعوة للانضمام إلى دائرة الثقة)، فيمكنك إزالة العضو من دائرة الثقة بإحدى الطرق التالية:

- من طريقة عرض Trust Circle، انقر فوق أو اضغط على **Your Trust Circles** (دوائر الثقة الخاصة بك)، ثم انقر نقرًا مزدوجًا فوق أو اضغط مرتين على دائرة الثقة لعرض قائمة الأعضاء الحاليين. انقر فوق أو اضغط على أيقونة **سلة المهملات** بجوار اسم العضو المراد إزالته.
- من طريقة عرض Trust Circle، انقر فوق أو اضغط على **Members** (الأعضاء)، ثم انقر نقرًا مزدوجًا فوق أو اضغط مرتين على العضو لعرض دوائر الثقة التي يعتبر عضوًا فيها. انقر فوق أو اضغط على أيقونة **سلة المهملات** بجوار دائرة ثقة لإزالة العضو من دائرة الثقة تلك.

حذف دائرة ثقة

تلزم الملكية لحذف دائرة الثقة.

▲ من طريقة عرض Trust Circle، انقر فوق أو اضغط على **Your Trust Circles** (دوائر الثقة الخاصة بك)، وانقر فوق أو اضغط على أيقونة **سلة المهملات** بجوار دائرة الثقة المراد حذفها.

يؤدي هذا الإجراء إلى حذف دائرة الثقة من الصفحة وإرسال رسائل بريد إلكتروني إلى جميع أعضاء دائرة الثقة تعلمهم بأنه تم حذف دائرة الثقة. يتم فك تشفير أية ملفات أو مجلدات كانت متضمنة في دائرة الثقة تلك.

تعيين التفضيلات

من طريقة عرض Trust Circle، انقر فوق أو اضغط على **Preferences** (التفضيلات). فيتم عرض ثلاث علامات تبويب.

- **Email Settings** (إعدادات البريد الإلكتروني)

الخيار	الوصف
Username (اسم المستخدم)	يتم عرض اسم المستخدم حاليًا. لتغيير اسم المستخدم، أدخل اسم مستخدم جديدًا في مربع النص. فيتم حفظ التغييرات تلقائيًا.
Email Address (عنوان البريد الإلكتروني)	يتم عرض حساب البريد الإلكتروني المستخدم حاليًا. لتغييره، انقر فوق أو اضغط على **Change Email Settings** (تغيير إعدادات البريد الإلكتروني)، ثم اتبع الإرشادات الظاهرة على الشاشة.
New Member Confirmation (تأكيد عضو جديد)	حدد من بين الخيارات التالية: ◦ **Confirm Automatically** (التأكيد تلقائيًا) — بعد تلقي قبول الدعوة من المدعو (المدعوين)، يتم تأكيد عضويته في دائرة الثقة دون أي إدخال يدوي، ويتم إرسال بريد إلكتروني للتأكيد إلى المدعو (المدعوين). ◦ **Confirm Manually** (التأكيد يدويًا) — بعد تلقي قبول الدعوة من المدعو (المدعوين)، يلزم الإدخال اليدوي لتسجيل الأعضاء الجدد داخل دائرة الثقة، ثم يتم إرسال بريد إلكتروني للتأكيد إلى المدعو (المدعوين). ◦ **Require Verification** (يلزم التحقق) — بعد تلقي قبول الدعوة من المدعو (المدعوين)، يلزم توفر رمز تحقق لتسجيل المدعو (المدعوين) بشكل كامل. يجب على مالك دائرة الثقة الاتصال بالمدعو (بالمدعوين) والحصول على رمز التحقق منهم. بعد إدخال الرمز الصحيح، يتم إرسال رسائل بريد إلكتروني للتأكيد.

الخيار	الوصف
Periodic Authentication (المصادقة الدورية)	تتطلب المصادقة الدورية من المستخدم إدخال كلمة مرور Windows بعد المهلة المحددة (مسجلة بالدقائق) وأيضًا أثناء تنفيذ العمليات الحساسة. ويسمح هذا الإعداد للمستخدمين بتشغيل المصادقة أو إيقاف تشغيلها.
Authentication Timeout (مهلة المصادقة)	حدد الفترة الزمنية للمهلة (مسجلة بالدقائق) قبل أن تلزم المصادقة.
Don't show confirmation message (عدم عرض رسالة التأكيد)	حدد خانة الاختيار لتعطيل عرض رسائل التأكيد، أو ألغِ تحديد خانة الاختيار لعرض رسائل التأكيد.
I'd like to help improve the HP Trust Circle through anonymous usage tracking (أرغب في المساعدة في تحسين HP Trust Circle عبر تعقب الاستخدام مجهول المصدر)	حدد خانة الاختيار للمشاركة في البرنامج، أو ألغِ تحديد خانة الاختيار في حالة عدم رغبتك في المشاركة.

- **Backup/Restore** (نسخ احتياطي/استعادة)

الخيار	الوصف
نسخ احتياطي	لنسخ بيانات تطبيق Trust Circle Manager/Reader (الإعدادات ودوائر الثقة) إلى ملف النسخة الاحتياطية. في حالة حدوث تعطل أو فشل النظام، يمكنك استخدام هذا الملف لاستعادة التثبيت الجديد لتطبيق Trust Circles إلى الحالة المحفوظة في الملف. **ملاحظة:** يتم حفظ بيانات تطبيق Trust Circle الخاصة بك فقط (دوائر الثقة والإعدادات والأعضاء). ولا يتم إجراء نسخ احتياطي للملفات الفعلية في مجلدات دوائر الثقة. ومن ثم ينبغي إجراء النسخ الاحتياطي لتلك الملفات بصورة منفصلة. لإجراء النسخ الاحتياطي لبيانات المستخدم والإعدادات في Trust Circle: ١. انقر فوق أو اضغط على **Backup** (نسخ احتياطي). ٢. اختر اسم ملف ودليلاً لملف النسخة الاحتياطية، ثم انقر فوق أو اضغط على **Save** (حفظ). ٣. أدخل كلمة مرور وأكدها، ثم انقر فوق أو اضغط على **OK** (موافق). ستكون كلمة المرور هذه مطلوبة لاستعادة هذا الملف.
استعادة	لاستعادة الإعدادات ودوائر الثقة من ملف النسخة الاحتياطية، وذلك عادة بعد تعطل النظام أو الترحيل إلى جهاز كمبيوتر آخر. لاستعادة إعدادات Trust Circle Manager وبيانات المستخدم: ١. انقر فوق أو اضغط على **Restore** (استعادة). ٢. انتقل إلى الدليل واسم الملف الخاصين بملف النسخة الاحتياطية، ثم انقر فوق أو اضغط على **Open** (فتح). ٣. أدخل كلمة المرور التي تم إعدادها أثناء إجراء النسخ الاحتياطي.

- **About** (نبذة عن) — يتم عرض إصدار برنامج Trust Circle Manager/Reader. كما يتم عرض الروابط للسماح بترقية Trust Circle Manager إلى الإصدار Pro أو لعرض بيان خصوصية HP.

٩ Theft recovery (طُرز محددة فقط)

يسمح لك Computrace (يتم شراؤه بشكل منفصل) بمراقبة جهاز الكمبيوتر وإدارته وتتبعه عن ُبعد.

بمجرد تنشيط Computrace، يتم تكوينه من مركز عملاء Absolute Software Customer Center. من مركز العملاء، يمكن للمسؤول تكوين Computrace لمراقبة أو إدارة الكمبيوتر. في حالة فقد الجهاز أو سرقته، يمكن لمركز العملاء مساعدة السلطات المحلية في تحديد مكان جهاز الكمبيوتر واستعادته. في حالة تكوين Computrace، فيمكنه أن يستمر في العمل حتى لو تم مسح محرك القرص الثابت أو استبداله.

لتنشيط Computrace:

١. اتصل بالإنترنت.

٢. افتح HP Client Security. للحصول على مزيد من المعلومات، انظر فتح HP Client Security في صفحة ٧.

٣. انقر فوق **Theft Recovery**.

٤. لتشغيل معالج تنشيط Computrace، انقر فوق **Get Started** (بدء التشغيل).

٥. أدخل معلومات الاتصال ومعلومات الدفع لبطاقة ائتمانك، أو أدخل مفتاح المنتج الذي سبق شراؤه.

يقوم معالج التنشيط بمعالجة العملية بأمان وينشئ حساب المستخدم الخاص بك على موقع ويب Absolute Software Customer Center. وفور الاكتمال، تتلقى رسالة تأكيد بالبريد الإلكتروني تحتوي على معلومات حسابك في خدمة العملاء.

إذا كنت قد قمت مسبقًا بتشغيل معالج تنشيط Computrace ولديك حساب مستخدم مركز العملاء مسبقًا، يمكنك شراء تراخيص إضافية عن طريق الاتصال بممثل حساب HP.

لتسجيل الدخول إلى مركز العملاء:

١. انتقل إلى .

٢. في حقلي **Login ID** (معرف تسجيل الدخول) و**Password** (كلمة المرور)، أدخل بيانات الاعتماد التي وردت في رسالة التأكيد بالبريد الإلكتروني، ثم انقر فوق **Log in** (تسجيل الدخول).

من خلال استخدام مركز العملاء، يمكنك:

- مراقبة أجهزة الكمبيوتر الخاصة بك.
- حماية بياناتك البعيدة.
- الإبلاغ عن سرقة أي جهاز كمبيوتر محمي بواسطة Computrace.

▲ انقر فوق **Learn More** (معرفة المزيد) لمزيد من المعلومات حول Computrace.

١٠ استثناءات كلمة المرور المترجمة

عند مستوى المصادقة عند بدء التشغيل ومستوى HP Drive Encryption، تكون إتاحة استخدام كلمة المرور المترجمة أمرًا مقيدًا. للحصول على مزيد من المعلومات، انظر محررات IME لنظام Windows غير المعتمدة عند مستوى المصادقة عند بدء التشغيل أو مستوى Drive Encryption في صفحة ٤٩.

ما يجب فعله عند رفض كلمة مرور

يمكن رفض كلمات المرور للأسباب التالية:

- هناك مستخدم يستخدم محرر IME غير معتمد. وهذه مشكلة شائعة مع اللغات مزدوجة البايت (الكورية، اليابانية، الصينية). لحل هذه المشكلة:

١. باستخدام **Control Panel** (لوحة التحكم)، أضف تخطيط لوحة مفاتيح معتمدًا (أضف لوحات المفاتيح الإنجليزية/الولايات المتحدة أسفل لغة الإدخال الصينية).

٢. قم بتعيين لوحة المفاتيح المعتمدة على الإدخال الافتراضي.

٣. ابدأ تشغيل HP Client Security، ثم أدخل كلمة مرور Windows.

- هناك مستخدم يستخدم حرفًا غير معتمد. لحل هذه المشكلة:

١. غيّر كلمة مرور Windows بحيث لا تستخدم سوى الأحرف المعتمدة. للحصول على مزيد من المعلومات حول الأحرف غير المعتمدة، انظر معالجة المفتاح الخاصة في صفحة ٥٠.

٢. ابدأ تشغيل HP Client Security، ثم أدخل كلمة مرور Windows.

محررات IME لنظام Windows غير المعتمدة عند مستوى المصادقة عند بدء التشغيل أو مستوى Drive Encryption

في نظام Windows، يمكن أن يختار المستخدم IME (محرر أسلوب الإدخال) لإدخال حروف ورموز معقدة مثل الحروف اليابانية أو الصينية، من خلال استخدام لوحة المفاتيح الغربية القياسية.

ومحررات IME غير معتمدة عند مستوى المصادقة عند بدء التشغيل أو مستوى Drive Encryption. لا يمكن إدخال كلمة مرور Windows باستخدام محرر IME في شاشة تسجيل دخول المصادقة عند بدء التشغيل أو HP Drive Encryption، وقد يؤدي القيام بذلك إلى حالة التأمين. في بعض الحالات، فإن Microsoft® Windows لا يعرض محرر IME عندما يدخل المستخدم كلمة المرور.

الحل هو الانتقال إلى أحد تخطيطات لوحة المفاتيح المعتمدة التالية التي تترجم إلى تخطيط لوحة المفاتيح ٠٠٠٠٠٤١١:

- محرر Microsoft IME للغة اليابانية
- تخطيط لوحة مفاتيح اللغة اليابانية
- محرر IME Office 2007 للغة اليابانية — إذا استخدمت شركة Microsoft أو جهة خارجية مصطلح IME أو محرر أسلوب الإدخال، فقد لا يكون أسلوب الإدخال IME بالفعل. ويمكن أن يتسبب ذلك في الالتباس، ولكن البرنامج يقرأ تمثيل الرمز السداسي العشري. وبالتالي، إذا كان IME يعين تخطيط لوحة مفاتيح معتمدة، فعندئذٍ يمكن لبرنامج HP Client Security إتاحة استخدام التكوين.

⚠ **تحذير!** في حالة نشر HP Client Security، يتم رفض كلمات المرور التي يتم إدخالها بواسطة Windows IME.

تغيير كلمة المرور باستخدام تخطيط لوحة المفاتيح المعتمدة أيضًا

إذا تم تحديد كلمة المرور في البداية بواسطة تخطيط لوحة مفاتيح واحد، مثل الإنجليزية للولايات المتحدة (٤٠٩)، وبعد ذلك غيَّر المستخدم كلمة المرور باستخدام تخطيط لوحة مفاتيح مختلف ومعتمد أيضًا، مثل الأمريكية اللاتينية (080A)، فسينجح تغيير كلمة المرور في HP Drive Encryption، ولكنه سيخفق في نظام BIOS في حال استخدام المستخدم حروفًا موجودة في لوحة المفاتيح الأخيرة وليست في الأولى (على سبيل المثال، ē).

ملاحظة: يمكن للمسؤولين حل هذه المشكلة باستخدام صفحة مستخدمي HP Client Security (والتي يتم الوصول إليها من أيقونة **Gear** (الترس) بالصفحة الرئيسية) لإزالة المستخدم من HP Client Security، وتحديد تخطيط لوحة المفاتيح المراد في نظام التشغيل، ثم تشغيل معالج إعداد HP Client Security مرة أخرى للمستخدم نفسه. يخزن نظام BIOS تخطيط لوحة المفاتيح المرغوب ويتم تعيين كلمات المرور التي يمكن كتابتها باستخدام تخطيط لوحة المفاتيح هذا بصورة صحيحة في BIOS.

ومن المشكلات الأخرى المحتملة استخدام تخطيطات لوحة مفاتيح مختلفة يمكن أن تكتب جميعها الحروف نفسها. على سبيل المثال، يمكن لكل من تخطيط لوحة المفاتيح الدولية الأمريكية (٢٠٤٠٩) وتخطيط لوحة المفاتيح الأمريكية اللاتينية (080A) كتابة الحرف é، بالرغم من أنه قد يلزم الضغط على تسلسلات مفاتيح مختلفة. إذا تم تحديد كلمة مرور في البداية بواسطة تخطيط لوحة المفاتيح الأمريكية اللاتينية، فعندئذٍ يتم تعيين تخطيط لوحة المفاتيح الأمريكية اللاتينية في نظام BIOS، حتى وإن تم تغيير كلمة المرور بعد ذلك باستخدام تخطيط لوحة المفاتيح الدولية الأمريكية.

معالجة المفتاح الخاصة

- الصينية، السلوفاكية، الفرنسية الكندية، التشيكية

عندما يحدد مستخدم أحد تخطيطات لوحات المفاتيح السابقة، ثم يُدخِل كلمة مرور (مثل، abcdef)، يجب إدخال كلمة المرور نفسها أثناء الضغط على مفتاح shift للأحرف الصغيرة ومفتاح shift وcaps lock للأحرف الكبيرة في المصادقة عند بدء التشغيل وHP Drive Encryption. ويجب إدخال كلمات المرور الرقمية باستخدام لوحة المفاتيح الرقمية.

- الكورية

عندما يحدد مستخدم تخطيط لوحة مفاتيح كورية معتمدة، ثم يُدخِل كلمة مرور، يجب إدخال كلمة المرور نفسها أثناء الضغط على مفتاح alt الأيمن للأحرف الصغيرة ومفتاح alt الأيمن وcaps lock للأحرف الكبيرة في المصادقة عند بدء التشغيل وHP Drive Encryption.

- يعرض الجدول التالي الأحرف غير المعتمدة:

اللغة	Windows	BIOS	Drive Encryption
العربية	ينتج الضغط على المفاتيح "لإ" و"لآ" و"لا" حرفين.	ينتج الضغط على المفاتيح "لإ" و"لآ" و"لا" حرفًا واحدًا.	ينتج الضغط على المفاتيح "لإ" و"لآ" و"لا" حرفًا واحدًا.
الفرنسية الكندية	ç è à ù é مع استخدام مفتاح caps lock تكون Ç È À Ù É في Windows.	ç è à ù é مع استخدام مفتاح caps lock تكون ç è à ù é في المصادقة عند بدء التشغيل.	ç è à ù é مع استخدام مفتاح caps lock تكون ç è à ù é في HP Drive Encryption.
الإسبانية	لا يتم دعم 40a. وبالرغم من ذلك يمكن استخدامه؛ لأن البرنامج يحوله إلى c0a. لكن، يوصى بأن يغير المستخدمون المتحدثون باللغة الإسبانية تخطيط لوحة مفاتيح Windows إلى 1040a (شكل مختلف من الإسبانية) أو 080a (أمريكية لاتينية)، نظرًا للاختلافات الدقيقة بين تخطيطات لوحة المفاتيح.	غير متوفر	غير متوفر

اللغة	Windows	BIOS	Drive Encryption
الأمريكية الدولية	◦ يتم رفض المفاتيح ¡ و¤ و‘ و’ و¥، و× في الصف العلوي. ◦ يتم رفض المفاتيح å و® و Þ في الصف الثاني. ◦ يتم رفض المفاتيح á و ð و ø في الصف الثالث. ◦ يتم رفض المفتاح æ في الصف السفلي.	غير متوفر	غير متوفر
التشيكية	◦ يتم رفض المفتاح ğ. ◦ يتم رفض المفتاح į. ◦ يتم رفض المفتاح ų. ◦ يتم رفض المفاتيح ė و ı و ž. ◦ يتم رفض المفاتيح ģ و ķ و ļ و ņ و ţ.	غير متوفر	غير متوفر
السلوفاكية	يتم رفض المفتاح ž.	◦ يتم رفض المفاتيح š و ś و ş عند الكتابة، ولكن يتم قبولها عند إدخالها بواسطة لوحة المفاتيح على الشاشة. ◦ ينتج الضغط على مفتاح ţ الهامد حرفين.	غير متوفر
المجرية	يتم رفض المفتاح ž.	ينتج الضغط على مفتاح ţ حرفين.	غير متوفر
السلوفينية	يتم رفض المفتاح Ž في Windows، وينتج الضغط على المفتاح alt مفتاحا هامدًا في نظام BIOS.	يتم رفض المفاتيح ú و Ú و ű و Ű و ş و Ş و ś و Ś و š و Š في نظام BIOS.	غير متوفر
اليابانية	يكون Microsoft Office 2007 IME اختيارًا أفضل عندما يتوفر. بالرغم من اسم IME، فإن تخطيط لوحة المفاتيح ٤١١ هو المعتمد بالفعل.	غير متوفر	غير متوفر

مسرد

Bluetooth
التقنية التي تستخدم عمليات الإرسال اللاسلكي لتمكين أجهزة الكمبيوتر والطابعات وأجهزة الماوس والهواتف المحمولة التي تم تمكين ميزة Bluetooth بها وغيرها من أجهزة الاتصال اللاسلكي عبر مسافة قصيرة.

Drive Encryption
يحمي بياناتك من خلال تشفير محرك (محركات) القرص الثابت، مما يجعل المعلومات غير قابلة للقراءة من ِقبل أولئك الذين لا يملكون التصريح اللازم.

DriveLock
ميزة أمان تربط محرك القرص الثابت بمستخدم وتطلب من المستخدم كتابة كلمة مرور DriveLock بشكل صحيح عند بدء تشغيل الكمبيوتر.

PKI
معيار البنية التحتية للمفتاح العام الذي يعرف واجهات إنشاء واستخدام وإدارة الشهادات ومفاتيح التشفير.

Trust Circle
يوفر وسيلة لاحتواء البيانات من خلال ربط البيانات بمجموعة معينة من المستخدمين الموثوق فيهم. ويؤدي هذا إلى منع وقوع البيانات في أيدي أشخاص غير موثوق فيهم سواء عن طريق الصدفة أم بصورة متعمدة. ومن خلال الحماية بتقنية CryptoMill's Zero Overhead Key Management، تكون البيانات مقصورة بصورة مشفرة على دائرة ثقة. ومن ثم تمنع هذه الميزة فك تشفير المستندات أو المعلومات الحساسة الأخرى خارج دائرة الثقة.

Trust Circle Manager/Reader
لا يقبل برنامج Trust Circle Reader سوى الدعوات المرسلة من مستخدمي Trust Circle Manager. ولكن يسمح Trust Circle Manager بإنشاء دوائر ثقة. وتتضمن الميزات دعوة شخص ما عبر البريد الإلكتروني إلى دائرة ثقة وقبول دعوات دوائر الثقة من الآخرين. بمجرد إنشاء دائرة ثقة بين نظراء، يمكن بأمان مشاركة الملفات المحمية بدائرة الثقة تلك.

أرشيف الاستعادة في حالات الطوارئ
منطقة تخزين محمية تسمح بإعادة تشفير مفاتيح المستخدم الأساسية من مفتاح مالك نظام أساسي إلى آخر.

أسلوب تسجيل الدخول الآمن
أسلوب تسجيل الدخول إلى الكمبيوتر.

أصل
مكون بيانات يتألف من معلومات شخصية أو ملفات أو بيانات محفوظات وبيانات مرتبطة بالويب، وهكذا، ويتم تخزينه على محرك القرص الثابت.

إتلاف تلقائي
الإتلاف الذي تقوم بتحديد موعده في File Sanitizer.

إتلاف يدوي
الإتلاف الفوري لأصل أو أصول محددة والذي يتجاوز عمليات الإتلاف المحددة بالجدول.

إعادة التمهيد
عملية إعادة تشغيل الكمبيوتر.

استعادة
عملية تنسخ معلومات البرنامج من ملف نسخة احتياطية تم حفظها مسبقًا إلى داخل هذا البرنامج.

الإتلاف
تنفيذ خوارزمية تكتب بيانات لا معنى لها فوق البيانات المتضمنة في الأصل.

الاسترداد من خلال HP SpareKey
القدرة على الوصول إلى جهاز الكمبيوتر الخاص بك عن طريق الإجابة عن أسئلة الحماية بشكل صحيح.

البطاقة الذكية
جهاز يمكن استخدامه مع رمز PIN للمصادقة.

التشفير

إجراء شبيه باستخدام الخوارزمية، ُيستخدم في التشفير لتحويل النص العادي إلى نص مشفر لمنع المستلمين غير المصرح لهم من قراءة تلك البيانات. وهناك العديد من أنواع تشفير البيانات، وهي الأساس لحماية الشبكات. وتشمل الأنواع الشائعة مقياس تشفير البيانات وتشفير المفتاح العام.

الصفحة الرئيسية
موقع مركزي حيث يمكنك الوصول إلى الميزات والإعدادات في HP Client Security وإدارتها.

المجموعة
مجموعة المستخدمين الذين لديهم مستوى الوصول أو رفض الوصول نفسه إلى فئة جهاز أو إلى جهاز بعينه.

المسؤول
انظر مسؤول *Windows*.

المصادقة عند التشغيل
ميزة حماية تتطلب شكلاً من أشكال المصادقة، مثل بطاقة ذكية، ورقاقة حماية، أو كلمة المرور، عندما يتم تشغيل الكمبيوتر.

المصادقة في الوقت المناسب
راجع تعليمات برنامج HP Device Access Manager.

النسخ الاحتياطي
استخدام ميزة النسخ الاحتياطي لحفظ نسخة من معلومات البرنامج المهمة بموقع خارج البرنامج. ويمكن استخدامها بعد ذلك لاستعادة المعلومات في وقت لاحق على الكمبيوتر نفسه أو كمبيوتر آخر.

الهوية
في HP Client Security، مجموعة من بيانات الاعتماد والإعدادات التي يتم التعامل معها كحساب أو ملف تعريف لمستخدم معين.

بصمة الإصبع
استخراج رقمي لصورة بصمة إصبعك. ولا يتم تخزين صورة بصمة إصبعك الحقيقية مطلًقا بواسطة تطبيق HP Client Security.

بطاقة ID
أداة في سطح مكتب Windows تعمل على التحديد البصري لسطح مكتبك عن طريق اسم المستخدم الخاص بك وصورتك المختارة.

بطاقة الاقتراب
بطاقة بلاستيكية تتضمن رقاقة كمبيوتر يمكن استخدامها للمصادقة بالإضافة إلى بيانات الاعتماد الأخرى لتوفير حماية إضافية.

بطاقة بدون موصلات
بطاقة بلاستيكية تتضمن رقاقة كمبيوتر يمكن استخدامها للمصادقة.

بيانات الاعتماد
معلومة معينة أو جهاز يستخدم لمصادقة مستخدم فردي.

تسجيل الدخول
كائن داخل تطبيق HP Client Security يتكون من اسم مستخدم وكلمة مرور (ومن الممكن أن تكون هناك معلومات أخرى محددة) ويمكن استخدامه لتسجيل الدخول إلى مواقع الويب والبرامج الأخرى.

تسجيل دخول موحد
ميزة تخزن معلومات المصادقة وتتيح لك استخدام HP Client Security للوصول إلى الإنترنت وتطبيقات Windows التي تتطلب مصادقة كلمة المرور.

تشفير الأجهزة
استخدام محركات الأقراص ذاتية التشفير التي تستوفي مواصفات Trusted Computing Group's OPAL لإدارة محرك الأقراص ذاتي التشفير لإكمال التشفير الفوري. وتشفير الأجهزة هو إجراء فوري وقد يستغرق فقط دقائق معدودة، لكن تشفير البرامج قد يستغرق ساعات عديدة.

تشفير البرامج
هو استخدام برنامج لتشفير محرك القرص الثابت، مقطًعا بمقطع. وهذه العملية أبطأ من تشفير الأجهزة.

تقليل المساحة الحرة
كتابة بيانات عشوائية فوق الأصول المحذوفة والمساحة غير المستخدمة. تحد هذه العملية من وجود الأصل المحذوف بحيث يصعب كثيًرا استرداد الأصل الأصلي.

تنشيط
المهمة التي يجب إكمالها قبل أن تصبح أي من ميزات Drive Encryption قابلة للوصول إليها. ويمكن للمسؤولين تنشيط Drive Encryption باستخدام معالج إعداد برنامج HP Client Security أو HP Client Security. وتتكون عملية التنشيط من تنشيط البرنامج وتشفير محرك القرص وإنشاء مفتاح التشفير الاحتياطي الأولي على جهاز تخزين قابل للإزالة.

جهاز متصل
جهاز متصل بمنفذ بالكمبيوتر.

حساب شبكة
حساب مستخدم أو مسؤول Windows إما على كمبيوتر محلي، أو في مجموعة عمل، أو في مجال.

حساب مستخدم Windows
مستخدم مخول بتسجيل الدخول إلى شبكة أو كمبيوتر معين.

حل الشفرة
إجراء يستخدم في التشفير لتحويل البيانات المشفرة إلى نص عادي.

حماية تسجيل الدخول إلى Windows
يحمي حساب (حسابات) Windows من خلال المطالبة باستخدام بيانات اعتماد معينة للوصول.

رقاقة الحماية المضمنة للوحدة النمطية للنظام الأساسي الموثوق به (TPM)
يصادق TPM على الكمبيوتر، بدلاً من المستخدم، عن طريق تخزين معلومات خاصة بنظام المضيف، مثل مفاتيح التشفير، والشهادات الرقمية، وكلمات المرور. يقلل TPM من خطر انكشاف المعلومات على الكمبيوتر عن طريق السرقة المادية أو هجوم القراصنة الخارجيين.

رمز PIN
رقم تعريف شخصي لمستخدم مسجَّل لاستخدامه في المصادقة.

سياسة التحكم في الوصول إلى الأجهزة
قائمة الأجهزة المسموح للمستخدم بالوصول إليها أو تلك المرفوض وصوله إليها.

شاشة تسجيل الدخول إلى Drive Encryption
انظر "مصادقة ما قبل التمهيد في Drive Encryption".

فئة الجهاز
جميع الأجهزة من نوع معين، مثل محركات الأقراص.

مجال
مجموعة من أجهزة الكمبيوتر التي هي جزء من شبكة وتتشارك في قاعدة بيانات ذات دليل مشترك. وتتم تسمية المجالات بشكل فريد، ولكل منها مجموعة من القواعد والإجراءات المشتركة.

مجلد Trust Circle
أي مجلد محمي بدائرة ثقة.

مسؤول Windows
مستخدم يمتلك كامل الحقوق لتعديل الأذونات وإدارة حسابات المستخدمين الآخرين.

مستخدم
أي شخص يتم تسجيله في Drive Encryption. يمتلك المستخدمون غير المسؤولين حقوقًا محدودة في Drive Encryption. يمكنهم فقط التسجيل (بعد موافقة المسؤول) وتسجيل الدخول.

مصادقة
عملية التحقق من أنك الشخص الذي تدعي أنك هو، من خلال استخدام بيانات الاعتماد والتي تشمل كلمة مرور Windows أو بصمة الإصبع أو بطاقة ذكية أو بطاقة غير تلامسية أو بطاقة اقتراب.

مصادقة ما قبل التمهيد في Drive Encryption.
شاشة تسجيل الدخول التي يتم عرضها قبل بدء تشغيل Windows. يجب على المستخدمين إدخال اسم مستخدم Windows وكلمة المرور أو رمز PIN للبطاقة الذكية أو تمرير إصبع مسجل. إذا تم تحديد تسجيل الدخول بخطوة واحدة، فإن إدخال المعلومات الصحيحة في شاشة تسجيل الدخول إلى Drive Encryption يسمح لك بالوصول المباشر إلى Windows دون الحاجة إلى تسجيل الدخول مرة أخرى في شاشة تسجيل الدخول في Windows.

نظام ملفات التشفير (EFS)
نظام يقوم بتشفير جميع الملفات والمجلدات الفرعية ضمن المجلد المحدد.

الفهرس