HP ProtectTools

دليل المستخدم

الإصدار الأول: أوكتوبر 2009

رقم الجزء الخاص بالمستند: 572661-171

جدول المحتويات

١ مقدمة إلى الحماية

بوفر برنامج HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) ميزات حماية تساعد على الحماية من الوصول غير المصرح به إلى جهاز الكمبيوتر، وشبكات الاتصال، والبيانات الهامة. يمكن إدارة HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) من خلال ميزة Administrative Console (وحدة تحكم إدارية).

باستخدام وحدة التحكم، يمكن للمسؤول المحلي القيام بالمهام التالية:

- تمكين ميزات الحماية أو تعطيلها
- تسجيل بصمات أصابع مستخدمي هذا الكمبيوتر
- إعداد بطاقة ذكية
- تحديد بيانات الاعتماد اللازمة للمصادقة
- إدارة مستخدمي جهاز الكمبيوتر
- ضبط المعلمات الخاصة بالجهاز
- تكوين تطبيقات Security Manager (إدارة الحماية) المثبتة
- إضافة تطبيقات Security Manager (إدارة الحماية) إضافية

قد تختلف وحدات البرامج المتاحة لجهاز الكمبيوتر الخاص بك تبعًا للطراز.

يمكن تثبيت وحدات برنامج HP ProtectTools أو تحميلها بشكل مسبق أو تنزيلها من موقع HP على الويب. للحصول على مزيد من المعلومات، قم بزيارة http://www.hp.com.

ملاحظة: كتبت الإرشادات في هذا الدليل افتراضًا أنك قد ثبّتَ وحدات HP ProtectTools البرمجية النمطية القابلة التطبيق.

ميزات HP ProtectTools

يوضح الجدول التالي بالتفصيل الميزات الأساسية الخاصة بوحدات HP ProtectTools.

الوحدة النمطية	الميزات الأساسية
Credential Manager for HP ProtectTools (إدارة بيانات الاعتماد لـ HP ProtectTools)	• يعمل Password Manager (إدارة كلمة مرور) كوسيلة داعمة لكلمة المرور الشخصية حيث تيسر عملية تسجيل الدخول من خلال ميزة Single Sign On (تسجيل الدخول الموحد)، التي تتذكر بيانات اعتماد المستخدم تلقائيًا وتطبقها. • ويعزز Single Sign On (تسجيل الدخول الموحد) الحماية عن طريق المطالبة بتراكيب من تقنيات الحماية المختلفة, مثل بطاقة Java™ والتشخيص البيولوجي, للمصادقة على المستخدم. • تتم حماية تخزين كلمة المرور من خلال تشفير البرنامج ويمكن تعزيز الحماية باستخدام مصادقة جهاز الحماية، على سبيل المثال بطاقات Java أو المقاييس الحيوية. **ملاحظة:** وظائف Credential Manager (إدارة بيانات الاعتماد) موجودة تحت خيار Password Manager (إدارة كلمة مرور) الخاص بـ HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools)
Drive Encryption (تشفير محركات الأقراص) لـHP ProtectTools (طرز مختارة فقط)	• يوفر Drive Encryption (تشفير محركات الأقراص) تشفيرًا كليًا لمحرك القرص الثابت بأكمله. • ويجبر Drive Encryption (تشفير محركات الأقراص) المصادقة قبل التمهيد بغرض حل البيانات المشفرة وصولاً إليها.
Privacy Manager (إدارة الخصوصية) لـHP ProtectTools (طرز مختارة فقط)	• يستخدم Privacy Manager (إدارة الخصوصية) أساليب متقدمة في تسجيل الدخول للتحقق من مصدر الاتصال ومدى سلامته ودرجة حمايته وذلك عند استخدام البريد الإلكتروني أو مستندات Microsoft® Office أو الرسائل الفورية (IM).
File Sanitizer (أداة تعقيم الملفات) لـHP ProtectTools	• يتيح لك File Sanitizer (أداة تعقيم الملفات) تقطيع الأصول الرقمية بأمان (أي معلومات حساسة مثل ملفات التطبيقات ومحتويات السجل أو تلك المستندة إلى الويب أو معلومات حساسة أخرى) الموجودة في الكمبيوتر كما يتيح لك تبييض محرك الأقراص الثابت دوريًا.
Device Access Manager (إدارة الوصول إلى الأجهزة) لـHP ProtectTools (طرز مختارة فقط)	• تتيح Device Access Manager (إدارة الوصول إلى الأجهزة) لمديري تكنولوجيا المعلومات التحكم في الوصول إلى الأجهزة استنادًا إلى ملفات تعريف المستخدمين. • تمنع Device Access Manager (إدارة الوصول إلى الأجهزة) المستخدمين غير المصرح بهم من إزالة البيانات باستخدام وسائط تخزين خارجية ومن إدخال الفيروسات إلى النظام من الوسائط الخارجية. • يتمكن المسؤول من منع أشخاص معينة أو مجموعات المستخدمين من الوصول إلى الأجهزة القابلة الكتابة.

الوصول إلى أهداف الحماية الأساسية

تتمكن وحدات HP ProtectTools النمطية من التعامل لتوفر حلولاً لمشاكل الأمان المتنوعة, بما في ذلك أهداف الحماية الأساسية الآتية:

- الحماية من السرقة المستهدفة
- منع الوصول إلى البيانات الحساسة
- منع الوصول غير المصرح به من المواقع الداخلية أو الخارجية
- إنشاء سياسات كلمات مرور قوية
- تلبية مطالب الحماية التنظيمية

الحماية من السرقة المتعمدة

من أمثلة السرقة المتعمدة سرقة كمبيوتر يحتوي على بيانات ومعلومات العملاء السرية في واحدة من النقاط الأمنية بالمطار. الميزات التالية تساعد على الحماية من السرقة المتعمدة:

- وتساعد ميزة المصادقة قبل التمهيد, في حالة تمكينها, في منع الوصول إلى نظام التشغيل. راجع الإجراءات التالية:
  - Security Manager (إدارة الحماية)
  - Drive Encryption (تشفير محركات الأقراص)

وضع قيودًا على الوصول إلى البيانات الحساسة

نفترض أن هناك مراجع للعقود يعمل في إحدى المواقع وتم تزويده بكمبيوتر كي يتمكن من مراجعة بيانات مالية هامة، وكنت ترغب في عدم السماح للمراجع بطباعة الملفات أو حفظها على وسيلة يمكن النسخ عليها مثل قرص مضغوط. تساعد الميزات التالية على تقييد الوصول إلى البيانات:

- يسمح Device Access Manager (إدارة الوصول إلى الأجهزة) الخاص بـ HP ProtectTools لمديري أقسام تكنولوجيا المعلومات بتقييد الوصول إلى الأجهزة التي يمكن استخدامها في النسخ بحيث لا يمكن طباعة المعلومات الحساسة أو نسخها من محرك القرص الثابت إلى وسائط قابلة للإزالة.

منع الوصول غير المصرح به من المواقع الداخلية أو الخارجية

يمثل الوصول غير المصرح به إلى أجهزة الكمبيوتر الأعمالية غير المحمية خطرًا حقيقيًا على موارد شبكة المؤسسة مثل المعلومات من الخدمات المالية أو المدير التنفيذي أو طاقم البحث والتطوير وكذلك على الموارد الخاصة مثل سجل المرضى أو السجل المالي الشخصي. تساعد الميزات الآتية في منع الوصول غير المصرح به:

- وتساعد ميزة المصادقة قبل التمهيد, في حالة تمكينها, في منع الوصول إلى نظام التشغيل. راجع الإجراءات التالية:
  - Password Manager (إدارة كلمة مرور)
  - Drive Encryption (تشفير محركات الأقراص)
- يضمن Password Manager (إدارة كلمة مرور) عدم حصول المستخدم غير المصرح له على كلمات المرور أو الوصول إلى التطبيقات المحمية بكلمات مرور.
- يسمح Device Access Manager (إدارة الوصول إلى الأجهزة) الخاص بـ HP ProtectTools لمديري أقسام تكنولوجيا المعلومات بتقييد الوصول إلى الأجهزة التي يمكن استخدامها في النسخ بحيث لا يمكن نسخ المعلومات الحساسة من محرك القرص الثابت.
- يساعد DriveLock على ضمان عدم الوصول إلى البيانات حتى إذا تمت إزالة القرص الصلب وتثبيته في نظام غير محمي.

إنشاء سياسات كلمات مرور قوية

إذا دعت الحاجة إلى استخدام سياسة كلمة مرور قوية للعديد من التطبيقات المعتمدة على الويب وقواعد البيانات، يقدم Security Manager (إدارة الحماية) مخزنًا محميًا يحتوي على كلمات المرور مما يساعد على تسجيل الدخول الموحد بيسر وسهولة

عناصر الحماية الإضافية

تعيين أدوار الحماية

إن إحدى الممارسات الهامة في إدارة حماية أجهزة الكمبيوتر (وخاصة في المنظمات الكبرى) هي تقسيم المسؤوليات والصلاحيات الخاصة بأنواع المسؤولين والمستخدمين المتنوعة.

ملاحظة: في المنظمات الصغيرة أو في حالة الاستخدام الشخصي, قد يقوم شخص واحد بهذه الأدوار كافة.

أما HP ProtectTools, فيمكن تقسيم مهام الحماية وصلاحياتها هذه إلى الأدوار الآتية:

- ضابط الحماية—يحدد مستوى حماية الشركة أو الشبكة ذلك ويحدد انتشار ميزات الحماية كبطاقات Java™ والقراء البيولوجية أو عملات USB.

ملاحظة: يمكن تخصيص العديد من الميزات في HP ProtectTools على يدي ضابط الحماية بالتعاون مع HP. للحصول على المزيد من المعلومات, راجع موقع الويب لـHP في http://www.hp.com.

- مسؤول تكنولوجيا المعلومات—هو الذي يطبق ميزات الحماية المحددة على يدي ضابط الحماية ويديرها. كما يمكنه تمكين بعض الميزات وتعطيلها. على سبيل المثال, إذا قرر ضابط الحماية انتهاج بطاقات Java, تمكن مسؤول تكنولوجيا المعلومات من تمكين وضع حماية الـBIOS الخاص ببطاقات Java.
- المستخدم—يستخدم ميزات الحماية. على سبيل المثال, إذا مكنا ضابط الحماية ومسؤول تكنولوجيا المعلومات بطاقات Java في النظام, تمكن المستخدم من تعيين الـPIN الخاص ببطاقة Java ومن استخدام البطاقة للمصادقة عليه.

تنبيه: يوصى بأن يقوم المسؤولون باتباع "أفضل الممارسات" في تقييد امتيازات المستخدم النهائي وتقييد وصول المستخدمين.

لا يجب منح المستخدمين غير المخولين امتيازات إدارية.

إدارة كلمات المرور الخاصة بـHP ProtectTools

تتم حماية معظم ميزات HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) من خلال كلمات المرور. يسرد الجدول التالي كلمات المرور الأكثر استخدامًا, وحدة البرنامج النمطية التي تضبط كلمات المرور فيها, ووظائف كلمات المرور.

كما تسرد في هذا الجدول كلمات المرور التي يتم تعيينها واستخدامها على يدي المسؤولين فقط. ويمكن تعيين كافة كلمات المرور الأخرى من قبل المستخدمين العاديين أو المسؤولين.

كلمة المرور لـHP ProtectTools	يتم تعيينها في وحدة HP ProtectTools النمطية هذه	الوظيفة
كلمة المرور الخاصة بتسجيل الدخول على Security Manager	Security Manager (إدارة الحماية)	تعرض كلمات المرور هذه خيارين: • يمكن استخدامها لتسجيل الدخول على Security Manager (إدارة الحماية) للوصول إلى Security Manager (إدارة الحماية) بعد تسجيل الدخول على Windows. • يمكن استخدامها للسماح بالوصول إلى Windows وSecurity Manager (إدارة الحماية) بشكل متزامن.
كلمة المرور الخاصة بملف استعادة Security Manager (إدارة الحماية)	Security Manager (إدارة الحماية)، بواسطة مسؤول تكنولوجيا المعلومات	تحمي الوصول إلى ملف استعادة Security Manager (إدارة الحماية).

كلمة المرور لـHP ProtectTools	يتم تعيينها في وحدة HP ProtectTools النمطية هذه	الوظيفة
PIN الخاص ببطاقة Java™	الحماية بواسطة بطاقة Java	حماية الوصول إلى محتويات بطاقة Java والمصادقة على مستخدمي بطاقة Java. وعند استخدامها للمصادقة وقت التشغيل, يحمي الـPIN الخاص ببطاقة Java أيضًا الوصول إلى الأداة المساعدة Computer Setup (إعداد الكمبيوتر) وإلى محتويات الكمبيوتر. المصادقة على مستخدمي Drive Encryption (تشفير محركات الأقراص), في حالة اختيار عملة بطاقة Java.
كلمة المرور الخاصة بتسجيل الدخول على Windows	لوحة تحكم Windows®	يمكن استخدامها لتسجيل الدخول يدويًا أو حفظها في بطاقة Java.

إنشاء كلمة مرور آمنة

عند إنشاء كلمات المرور، عليك باتباع المواصفات التي تم ضبطها بواسطة البرنامج أولاً. مع ذلك وبشكل عام, خذ بعين الاعتبار الإرشادات الآتية لتساعدك في إنشاء كلمات مرور قوية وفي تقليل فرص تعرض كلمات مرورك للسرقة:

- استخدام كلمات المرور الأطول من ستة أحرف وأفضل ما تكون أطول من ثمانية أحرف.
- خلط حالة أحرف كلمة المرور.
- وكلما أمكن ذلك, خلط الأحرف الأبجدية مع الرقمية وضمن فيها الأحرف الخاصة وعلامات الترقيم.
- استبدل أحرف الكلمات الأساسية بالأحرف الخاصة أو بالارقام. وعلى سبيل المثال, يمكنك استخدام الرقم 2 بدلاً من الحرف ؤ أو ئ.
- اجمع بين كلمات من لغتين مختلفة أو أكثر.
- اقطع كلمة أو جملة واضعًا الأرقام أو الأحرف الخاصة داخلها, على سبيل المثال, "ليلى2-2قط45."
- لا تستخدم كلمة مرور توجد في القواميس.
- لا تستخدم اسمك ككلمة مرور, كما لا تستخدم المعلومات الشخصية الأخرى, مثل تأريخ الميلاد أو أسماء الدلع, أو اسم البتولة, وحتى إذا عكست كتابته.
- غيّر كلمات المرور دوريًا. وقد تغيّر حرفين فقط.
- إذا دونت كلمة المرور, فلا تحتفظ بها في مكان جلي للعامة بالقرب من الكمبيوتر.
- لا تقم بحفظ كلمات المرور في ملف, مثل الرسائل الإلكترونية, على جهاز الكمبيوتر.
- لا تشارك الحسابات أو تفشي كلمات مرورك لأحد.

نسخ بيانات اعتماد HP ProtectTools احتياطيًا واستعادتها

يمكنك استخدام Drive Encryption (تشفير محركات الأقراص) الخاص بـ HP ProtectTools لتحديد بيانات اعتماد HP ProtectTools ونسخها احتياطيًا.

٢ بدء التشغيل

ملاحظة: إدارة HP ProtectTools تستلزم امتيازات إدارية.

يرشدك Setup Wizard (معالج إعداد) HP ProtectTools خلال إعداد أكثر ميزات Security Manager (إدارة الحماية) استخدامًا. ومع ذلك، توجد ثروة من الوظائف الإضافية التي يتيحها (وحدة تحكم إدارية لـ HP ProtectTools). يمكن تكوين نفس الإعدادات الموجودة في المعالج، بالإضافة إلى ميزات الحماية الإضافية، من خلال وحدة التحكم، التي يتم الوصول إليها من القائمة Start (ابدأ) الخاصة بـ Windows®. تنطبق هذه الإعدادات على الكمبيوتر وكل مستخدميه.

١. في صفحة Welcome (مرحبًا بك)، يمكنك تعطيل عرض المعالج باختيار أحد الخيارات.

٢. بعد مرور أسبوع على إعداد الكمبيوتر، أو عندما يمرر مستخدم يتمتع بالحقوق الإدارية أصبعه فوق جهاز قراءة بصمات الأصابع للمرة الأولى، سيبدأ معالج إعداد HP ProtectTools في العمل تلقائيًا لإرشادك عبر الخطوات الأساسية الخاصة بتكوين البرنامج. وسيبدأ برنامج فيديو تعليمي تلقائيًا حول إعداد الكمبيوتر الخاص بك.

٣. اتبع الإرشادات التي تظهر على الشاشة حتى يكتمل الإعداد.

إذا لم تكمل المعالج، سيتم تشغيله مرتين تلقائيًا. بعد ذلك، يمكنك الوصول إلى المعالج عبر بالون الإعلام الذي يظهر بالقرب من منطقة الإعلام الموجودة بشريط المهام (ما لم تكون قد عطلته كما هو موضوح في الخطوة 2 أعلاه) إلى أن يكتمل الإعداد.

لاستخدام تطبيقات HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools)، قم بتشغيل HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) من القائمة Start (ابدأ) أو انقر بزر الماوس الأيمن على الرمز Security Manager (إدارة الحماية) في منطقة الإعلام، التي تقع في أقصى يسار شريط المهام. HP ProtectTools Administrative Console (وحدة تحكم إدارية لـ HP ProtectTools) وتطبيقاتها متاحة لكل مستخدمي هذا الكمبيوتر.

فتح HP ProtectTools Administrative Console(وحدة تحكم إدارية لـ HP ProtectTools)

للقيام بالمهام الإدرارية مثل إعداد سياسات النظام أو تكوين البرنامج، افتح وحدة التحكم على النحو التالي:

- انقر فوق **Start (ابدأ)**، ثم **All Programs (كافة البرامج)**، ثم **HP**، ثم انقر فوق **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**.

– أو –

في اللوحة اليمنى من Security Manager (إدارة الحماية)، انقر فوق **Administration** (إدارة).

وبالنسبة لمهام المستخدمين، مثل تسجيل بصمات الأصابع أو استخدام Security Manager (إدارة الحماية)، افتح وحدة التحكم على النحو التالي:

- انقر فوق **Start (ابدأ)**، ثم **All Programs (كافة البرامج)**، ثم **HP**، ثم انقر فوق **HP ProtectTools Security Manager (إدارة الحماية لـHP ProtectTools)**.

– أو –

انقر نقرًا مزدوجًا فوق رمز **HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools)** في ناحية الإعلام، في أقصى يسار شريط المهام.

تمكين ميزات الحماية

سيطالبك Setup Wizard (معالج الإعداد) بتأكيد هويتك.

١. اقرأ المكتوب بشاشة "الترحيب" ثم انقر فوق **Next** (التالي).

٢. قم بتأكيد هويتك، سواء بكتابة كلمة مرور Windows الخاصة بك إذا لم يكن لديك أي بصمات أصابع مسجلة بعد، أو بمسح بصمات أصابعك باستخدام جهاز قراءة بصمات الأصابع. انقر فوق **Next (التالي)**.

إذا كانت كلمة مرور Windows الخاصة بك فارغة، فستتم مطالبتك بإنشاء واحدة. كلمة مرور Windows مطلوبة لحماية حساب Windows الخاص بك من وصول الأشخاص غير المصرح لهم، وكذلك لاستخدام ميزات HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools).

سيرشدك Setup Wizard (معالج الإعداد) عبر العملية الخاصة بتمكين ميزات الحماية التي تنطبق على كل مستخدمي الكمبيوتر:

- يعمل Windows Logon Security (حماية تسجيل الدخول على Windows) على حماية حساب (حسابات) Windows الخاصة بك حيث يطالب ببيانات اعتماد معينة للسماح بالوصول.
- يحمي Drive Encryption (تشفير محركات الأقراص) بياناتك عن طريق تشفير القرص (الأقراص) الصلب الخاصة بك، بحيث يعجز الأشخاص غير المصرح لهم عن قراءة المعلومات.
- يحمي Pre-Boot Security (الحماية ما قبل التمهيد) الكمبيوتر الخاص بك بحظر وصول الأشخاص غير المصرح لهم قبل إعادة تشغيل Windows.

لتمكين إحدى ميزات الحماية، حدد خانة الاختيار المقابلة. كلما حددت ميزات إضافية كلما صار الكمبيوتر أكثر أمانًا.

ملاحظة: لن Pre-Boot Security (الحماية ما قبل التمهيد) متاحًا في حالة دعم BIOS له.

تسجيل بصمات الأصابع الخاصة بك

إذا قمت بتحديد Fingerprint (بصمة الأصبع) وإذا كان الكمبيوتر يحتوي على جهاز قراءة بصمات أصابع مدمج أو متصل بجهاز من هذا النوع، فسيتم إرشادك عبر عملية إعداد أو "تسجيل" بصمات أصابعك:

١. يتم عرض رسم ليدين. يتم تمييز الأصابع المسجلة بالفعل باللون الأخضر. انقر الأصبع الموجود بالرسم.

ملاحظة: لحذف بصمة أصبع مسجلة من قبل، انقر فوق الأصبع المناظر.

٢. عند تحديدك لأصبع كي يتم تسجيله، فستتم مطالبتك بمسح بصمة هذا الأصبع حتى يتم تسجيله بنجاح. يتم تمييز الأصبع المسجل باللون الأخضر في الرسم.

٣. يجب أن تسجل أصبعين على الأقل، ومن المفضل أصبعي السبّابة أو الوسطى. كرر الخطوات من 1 إلى 3 للأصبع الأخر.

٤. انقر فوق **Next (التالي)**.

ملاحظة: عند تسجيل بصمات الأصابع من خلال عملية بدء التشغيل، لا يتم حفظ معلومات بصمة الأصبع حتى تنقر على **Next (التالي)**. إذا ظل الكمبيوتر غير نشط لبعض الوقت، أو إذا أغلقت لوحة المعلومات، **فلن يتم** حفظ التغييرات التي قمت بها.

إعداد بطاقة ذكية

إذا حددت "بطاقة ذكية" وإذا كان هناك جهاز قراءة بطاقات ذكية مدمج في الكمبيوتر الخاص بك أو متصل به، فسيطالبك Setup Wizard (معالج إعداد) HP ProtectTools بإعداد PIN (رقم التعريف الشخصي) الخاص بالبطاقة الذكية.

لإعداد رقم PIN الخاص ببطاقة ذكية:

١. على صفحة "إعداد بطاقة ذكية"، أدخل رقم PIN وقم بتأكيده.

يمكنك تغيير رقم PIN الخاص بك. قم بتقديم رقم PIN القديم ثم اختر رقمًا جديدًا.

٢. للمتابعة، انقر فوق **Next (التالي)**.

استخدام Administrative Console (وحدة التحكم الإدارية)

HP ProtectTools Administrative Console (وحدة تحكم إدارية لـ HP ProtectTools) هي المكان الأساسي لإدارة ميزات HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) وتطبيقاته.

تتكون وحدة التحكم من المكونات التالية:

- **الأدوات**—تعرض الفئات التالية لتكوين الحماية على الكمبيوتر الخاص بك:
  - **البداية**— تسمح لك بتحديد مهام الحماية التي سيتم القيام بها.
  - **النظام**—يسمح لك بتكوين ميزات الحماية والمصادقة للمستخدمين والأجهزة.
  - **التطبيقات**—تعرض الإعدادات العامة لتطبيقات HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) وSecurity Manager.
  - **البيانات**—تقدم قائمة موسعة بالارتباطات التي تصل بتطبيقات Security Manager (إدارة الحماية) التي تحمي بياناتك.
- **أدوات الإدارة**—تقدم معلومات حول الأدوات الإضافية. تعرض اللوحة الموجودة أدناه الاختيارات التالية:
  - **Setup Wizard HP ProtectTools** (معالج الإعداد لـ HP ProtectTools)—يرشدك خلال إعداد HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools).
  - **التعليمات**—تعرض ملف التعليمات، الذي يقدم معلومات حول Security Manager (إدارة الحماية) وتطبيقاته المثبتة مسبقًا. التعليمات الخاصة بالتطبيقات التي يمكن أن تضيفها موجودة ضمن هذه التطبيقات.
  - **حول**—تعرض المعلومات الخاصة HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools)، مثل رقم الإصدار وإشعار حقوق النشر.
- **الناحية الأساسية**—تعرض الشاشات الخاصة بالتطبيق.

لفتح HP ProtectTools Administrative Console (وحدة تحكم إدارية لـ HP ProtectTools)، انقر فوق **Start (ابدأ)**، انقر فوق **All Programs (كافة البرامج)**، انقر فوق **HP**، ثم انقر فوق **HP ProtectTools Administrative Console** (وحدة تحكم إدارية لـ HP ProtectTools).

٣ تكوين النظام الخاص بك

يتم الوصول إلى مجموعة النظام من خلال Tools menu panel (لوحة قائمة الأدوات) في الجانب الأيمن من شاشة HP ProtectTools Administrative Console (وحدة تحكم إدارية لـ HP ProtectTools). يمكنك استخدام التطبيقات الموجودة بهذه المجموعات لإدارة السياسات والإعدادات للكمبيوتر ومستخدميه والأجهزة الخاصة به.

التطبيقات التالية موجودة ضمن مجموعة النظام:

- **الحماية**—يقوم بإدارة الميزات والمصادقة والإعدادات التي تحكم كيفية تعامل المستخدمين مع هذا الكمبيوتر.
- **المستخدمون**—يقوم بإعداد مستخدمي هذا الكمبيوتر وإدارتهم وتسجيلهم.
- **الأجهزة**—يقوم بإدارة الإعدادات الخاصة بأجهزة الحماية المدمجة بالكمبيوتر أو المتصلة به.

إعداد المصادقة للكمبيوتر

يمكنك، داخل تطبيق المصادقة، تحديد أي من ميزات الحماية يجب تطبيقها على هذا الكمبيوتر بالإضافة إلى إعداد السياسات التي تحكم الوصول إلى الكمبيوتر وتكوين الإعدادات الإضافية المتقدمة. يمكنك تحديد معلومات الاعتماد المطلوبة لتصديق كل فئة من المستخدمين عند تسجيل الدخول على Windows أو تسجيل الدخول على مواقع الويب والبرامج أثناء جلسة عمل المستخدم.

لإعداد المصادقة على الكمبيوتر الخاص بك:

١. في قائمة Security panel (لوحة الحماية)، انقر فوق **Authentication (مصادقة)**.

٢. لتكوين المصادقة على تسجيل الدخول، انقر فوق علامة التبويب **Logon Policy (سياسة تسجيل الدخول)**، قم بالتغييرات وانقر فوق **Apply (تطبيق)**.

٣. لتكوين المصادقة على الجلسة، انقر فوق علامة التبويب **Session Policy (سياسة الجلسة)**، قم بالتغييرات وانقر فوق **Apply (تطبيق)**.

سياسة تسجيل الدخول

لتحديد السياسات التي تتحكم في بيانات الاعتماد المطلوبة للمصادقة على مستخدم عند تسجيل الدخول على Windows:

١. في القائمة Tools (أدوات)، انقر فوق **Security (حماية)**، وانقر فوق **Authentication (مصادقة)**.

٢. في علامة التبويب **Logon Policy (سياسة تسجيل الدخول)**، انقر فوق فئة المستخدم.

٣. قم بتحديد معلومات اعتماد المصادقة المطلوبة لفئة المستخدم المحددة. يجب تحديد بيان اعتماد واحد على الأقل.

٤. حدد ما إذا كانت هناك حاجة لـ ANY (واحدة فقط) من بيانات الاعتماد المحددة أم ALL (لكل) البيانات للمصادقة على المستخدم. يمكنك أيضًا منع أي مستخدم من الوصول إلى الكمبيوتر.

٥. انقر فوق **Apply (تطبيق)**.

سياسة الجلسة

لتحديد السياسات التي تحكم بيانات الاعتماد اللازمة للوصول إلى تطبيقات HP ProtectTools أثناء جلسة Windows:

١. في القائمة Tools (أدوات)، انقر فوق **Security (حماية)**، وانقر فوق **Authentication (مصادقة)**.

٢. في علامة التبويب **Session Policy (سياسة الجلسة)**، انقر فوق فئة المستخدم.

٣. قم بتحديد معلومات اعتماد المصادقة المطلوبة لفئة المستخدم المحددة.

٤. حدد ما إذا كانت هناك حاجة لـ ANY (واحدة فقط) من بيانات الاعتماد المحددة أم ALL (لكل) البيانات للمصادقة على المستخدم. يمكن ألا تحتاج إلى مصادقة للوصول إلى برنامج HP ProtectTools.

٥. انقر فوق **Apply (تطبيق)**.

إعدادات

يمكنك السماح بإعداد حماية واحد أو أكثر من إعدادات الحماية التالية:

- **Allow One Step logon (السماح بتسجيل الدخول في خطوة واحدة)**—يسمح لمستخدمي هذا الكمبيوتر بتجاوز تسجيل الدخول على Windows إذا تمت المصادقة في BIOS أو بمستوى القرص المشفر.
- **Allow HP SpareKey authentication for Windows logon (السماح بمصادقة HP SpareKey لتسجيل الدخول على Windows)**—يسمح لمستخدمي هذا الكمبيوتر باستخدام ميزة HP SpareKey لتسجيل الدخول على Windows بغض النظر عن أي سياسة مصادقة أخرى يتطلبها Security Manager (إدارة الحماية).

لتحرير الإعدادات:

١. انقر لتمكين إعداد معين أو تعطيله.

٢. انقر فوق **Apply (تطبيق)** لحفظ التغييرات التي قمت بها.

إدارة المستخدمين

يمكنك مراقبة مستخدمي HP ProtectTools الموجودة على هذا الكمبيوتر وإدارتهم من داخل تطبيق المستخدمين.

يتم إدراج كل مستخدمي HP ProtectTools والتحقق منهم في مقابل السياسات الموضوعة من خلال Security Manager (إدارة الحماية) وما إذا كانوا قاموا بتسجيل بيانات الاعتماد المناسبة التي تسمح لهم بالوفاء بهذه السياسات.

لإضافة مستخدمين إضافيين، انقر فوق **Add** (إضافة).

لحذف مستخدم، انقر فوق المستخدم، ثم انقر فوق **Delete** (حذف).

لتسجيل بصمات الأصابع أو إعداد بيانات اعتماد إضافية للمستخدم، انقر فوق المستخدم، ثم انقر فوق **Enroll** (تسجيل).

لعرض السياسات الخاصة بمستخدم معين، حدد المستخدم، ثم انقر فوق **View Policies (عرض السياسات)**.

تحديد إعدادات الجهاز

داخل تطبيق الجهاز، يمكنك تحديد الإعدادات المتاحة لأي أجهزة حماية مدمجة أو متصلة يتعرف عليها HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools).

بصمات الأصابع

توجد ثلاث علامات تبويب بصفحة بصمات الأصابع: انتساب وحساسية ومتقدم.

انتساب

يمكنك اختيار الحد الأدنى والحد الأقصى من بصمات الأصابع المسموح لمستخدم بتسجيلها.

يمكنك أيضًا مسح كل البيانات من جهاز قراءة بصمات الأصابع.

⚠ **تحذير!** سيتم مسح كل بيانات بصمات الأصابع الخاصة بكل المستخدمين بما فيهم المسؤولين. إذا تطلبت سياسة تسجيل الدخول بصمات الأصابع فقط، فقد يتم منع كل المستخدمين من تسجيل الدخول على الكمبيوتر.

الحساسية

لضبط درجة الحساسية التي يستخدمها جهاز قراءة بصمات الأصابع عند مسحه لبصمات أصابعك، قم بتحريك مربع التمرير.

إذا لم يتم التعرف على بصمة الأصبع، قد يكون من الضروري استخدام إعداد حساسية أقل. يزيد الإعداد الأعلى من الحساسية للاختلافات في مرات مسح بصمة الأصبع ولذلك يقلل من إمكانية القبول الزائف. يوفر الإعداد المتوسط-العالي مزيجًا من الحماية والراحة.

خيارات متقدمة

يمكنك تكوين جهاز قراءة بصمات الأصابع بحيث يتم توفير الطاقة عندما يعمل الكمبيوتر بطاقة البطارية.

البطاقة الذكية

يمكنك تكوين الكمبيوتر بحيث يتم قفله تلقائيًا عند إزالة البطاقة الذكية. ومع ذلك، سيتم قفل الكمبيوتر فقط إذا تم استخدام البطاقة الذكية كبيانات اعتماد للمصادقة عند تسجيل الدخول على Windows. لن تؤدي إزالة بطاقة ذكية لم يتم استخدامها لتسجيل الدخول على Windows إلى قفل الكمبيوتر.

▲ قم بتحديد خانة الاختيار لتعطيل أو تمكين قفل الكمبيوتر عند إزالة البطاقة الذكية.

٤ تكوين التطبيقات الخاصة بك

يتم الوصول إلى مجموعة التطبيقات من خلال Security Applications menu panel (لوحة قائمة تطبيقات الحماية) في الجانب الأيمن من شاشة HP ProtectTools Administrative Console (وحدة تحكم إدارية لـ HP ProtectTools). يمكنك استخدام إعدادات لتخصيص سلوك تطبيقات HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) المثبتة.

لتحرير إعدادات التطبيق الخاصة بك:

١. في القائمة Tools (أدوات)، من مجموعة **Applications (التطبيقات)**، انقر فوق **Settings (الإعدادات)**.

٢. انقر لتمكين إعداد معين أو تعطيله.

٣. انقر فوق **Apply (تطبيق)** لحفظ التغييرات التي قمت بها.

علامة التبويب General (عام)

الإعدادات التالية متاحة في علامة التبويب العامة:

- **لا تقم بتشغيل معالج الإعداد للمسؤولين تلقائيًا**—حدد هذا الخيار لمنع فتح المعالج تلقائيًا عند تسجيل الدخول.
- **لا تقم بتشغيل معالج البدء للمستخدمين تلقائيًا**—حدد هذا الخيار لمنع إعداد المستخدم تلقائيًا عند تسجيل الدخول.

علامة تبويب Applications (تطبيقات)

يمكن أن تتغير الإعدادات المعروضة هنا عند إضافة تطبيقات جديدة إلى Security Manager (إدارة الحماية). الحد الأدنى من الإعدادات التي تظهر تلقائيًا هي كالتالي:

- **Security Manager**—تمكن تطبيق Security Manager (إدارة الحماية) لكل مستخدمي الكمبيوتر.
- **Enable the Discover more button (تمكين الزر اكتشف المزيد)**—يسمح لكل مستخدمي هذا الكمبيوتر بإضافة تطبيقات إلى HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) بالنقر فوق الزر **Discover more (اكتشف المزيد [+])**.

لإرجاع كل التطبيقات لإعدادات الشركة المصنعة لها، انقر فوق الزر **Restore Defaults (استعادة الافتراضيات)**.

٥ إضافة أدوات إدارة

قد تتاح تطبيقات إضافية لإضافة أدوات إدارة جديدة إلى Security Manager (إدارة الحماية). يمكن للمسؤول عن هذا الكمبيوتر تعطيل هذه الميزة من خلال تطبيق الإعدادات.

لإضافة أدوات إدارة إضافية، انقر فوق **Management tools [+] (أدوات الإدارة [+])**.

يمكنك الوصول إلى موقع ويب DigitalPersona للبحث عن التطبيقات الجديدة، أو يمكنك وضع جدول للتحديثات التلقائية.

HP ProtectTools Security Manager ٦

يسمح لك HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) بزيادة حماية الكمبيوتر الخاص بك بدرجة كبيرة.

يمكنك استخدام تطبيقات Security Manager (إدارة الحماية) المحملة مسبقًا وكذلك التطبيقات الإضافية المتاحة للتحميل الفوري من الويب:

- إدارة تسجيل الدخول وكلمات المرور
- تغيير كلمة مرور الخاص بنظام تشغيل Windows® بسهولة
- إعداد تفضيلات البرنامج
- استخدام بصمات الأصابع لمزيد من الحماية والراحة
- إعداد بطاقة ذكية للمصادقة
- نسخ بيانات البرنامج احتياطيًا واستعادتها
- إضافة المزيد من التطبيقات

إجراءات الإعداد

بدء التشغيل

يتم عرض HP ProtectTools Setup Wizard (معالج الإعداد لـ HP ProtectTools) تلقائيًا كصفحة افتراضية في HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) حتى اكتمال الإعداد.

لإعداد Security Manager (إدارة الحماية) ، اتبع هذه الخطوات:

ملاحظة: إذا لم يتوافر جهاز قراءة بصمات أصابع أو بطاقة ذكية، قم بالخطوات 1 و5 و6 فقط.

١. في صفحة "الترحيب"، انقر فوق **Next (التالي)**.

٢. تسرد الصفحة التالية أساليب المصادقة المتاحة على هذا الكمبيوتر. انقر فوق **Next (التالي)** للمتابعة.

٣. في الصفحة الخاصة بـ"تأكيد الهوية"، اكتب كلمة مرور Windows الخاصة بك، ثم انقر فوق **Next (التالي)**.

٤. انظر موضوع واحد أو أكثر من الموضوعات التالية تبعًا لتكوين الكمبيوتر الخاص بك.

- إذا كان جهاز قراءة بصمات الأصابع متاحًا، فراجع تسجيل بصمات الأصابع الخاصة بك في صفحة ٢٤.
- إذا كانت البطاقة الذكية متاحة، فراجع إعداد بطاقة ذكية في صفحة ٢٥.

٥. إذا لم تكن البطاقة الذكية أو جهاز قراءة بصمات الأصابع متاحًا، ستتم مطالبتك بإدخال كلمة مرور Windows الخاصة بك. يجب أن تستخدم كلمة المرور هذه في المستقبل كلما كانت المصادقة مطلوبة.

٦. في الصفحة الأخيرة من المعالج، انقر فوق **Finish (إنهاء)**.

يتم عرض لوحة المعلومات الخاصة بـ Security Manager (إدارة الحماية).

تسجيل معلومات الاعتماد

يمكنك استخدام الصفحة "My Identity" (هويتي) لتسجيل طرق المصادقة المتعددة أو بيانات الاعتماد. بعد تسجيلها، يمكنك استخدام هذه الطرق لتسجيل الدخول على Security Manager (إدارة الحماية).

تسجيل بصمات الأصابع الخاصة بك

إذا كان الكمبيوتر يحتوي على جهاز قراءة بصمات أصابع مدمج أو متصل بجهاز من هذا النوع، فسيقوم HP ProtectTools Setup Wizard (معالج الإعداد لـ HP ProtectTools) بإرشادك عبر عملية إعداد أو "تسجيل" بصمات أصابعك.

١. اقرأ المكتوب بشاشة "الترحيب" ثم انقر فوق **Next (التالي)**.

٢. قم بتأكيد هويتك، سواء بكتابة كلمة مرور Windows الخاصة بك إذا لم يكن لديك أي بصمات أصابع مسجلة بعد، أو بمسح بصمات أصابعك باستخدام جهاز قراءة بصمات الأصابع. انقر فوق **Next (التالي)**.

إذا كانت كلمة مرور Windows الخاصة بك فارغة، فستتم مطالبتك بإنشاء واحدة. كلمة مرور Windows مطلوبة لحماية حساب Windows الخاص بك من وصول الأشخاص غير المصرح لهم، وكذلك لاستخدام ميزات HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools).

٣. يتم عرض رسم ليدين. يتم تمييز الأصابع المسجلة بالفعل باللون الأخضر. انقر الأصبع الموجود بالرسم.

ملاحظة: لحذف بصمة أصبع مسجلة من قبل، انقر فوق بصمة الأصبع المناظرة.

٤. عند تحديدك لأصبع كي يتم تسجيله، فستتم مطالبتك بمسح بصمة هذا الأصبع حتى يتم تسجيله بنجاح. يتم تمييز الأصبع المسجل باللون الأخضر في الرسم.

٥. يجب أن تسجل أصبعين على الأقل، ومن المفضل أصبعي السبّابة أو الوسطى. كرر الخطوات 3 و4 للأصبع الأخر.

٦. انقر فوق **Next (التالي)**.

ملاحظة: عند تسجيل بصمات الأصابع من خلال عملية بدء التشغيل، لا يتم حفظ معلومات بصمة الأصبع حتى تنقر على **Next (التالي)**. إذا ظل الكمبيوتر غير نشط لبعض الوقت، أو إذا أغلقت لوحة المعلومات، **فلن يتم** حفظ التغييرات التي قمت بها.

تغيير كلمة مرور Windows

يسمح لك Security Manager (إدارة الحماية) بتغيير كلمة مرور Windows بشكل أكثر بساطة وسرعة من تغييرها من خلال لوحة تحكم Windows.

لتغيير كلمة مرور Windows، اتبع الخطوات التالية:

١. من لوحة معلومات Security Manager (إدارة الحماية)، انقر فوق **"My Identity" (هويتي)**، انقر فوق **Credentials (بيانات الاعتماد)**، ثم انقر فوق **Password (كلمة المرور)**.

٢. أدخل كلمة المرور الحالية الخاصة بك في مربع النص **Current Windows password (كلمة مرور Windows الحالية)**.

٣. اكتب كلمة مرور جديدة في مربع النص **New Windows password (كلمة مرور Windows الجديدة)**، ثم اكتبها مرة أخرى في مربع النص **Confirm new password (تأكيد كلمة المرور الجديدة)**.

٤. انقر فوق **Change (تغيير)** لتغيير كلمة المرور الحالية على الفور إلى كلمة مرور الجديدة التي ستدخلها.

إعداد بطاقة ذكية

إذا كان هناك جهاز قراءة بطاقات ذكية مدمج في الكمبيوتر الخاص بك أو متصل به، فسيطالبك Security Manager (إدارة الحماية) لإعداد PIN (رقم التعريف الشخصي) الخاص بالبطاقة الذكية.

- لإعداد PIN الخاص ببطاقة ذكية - في صفحة Set up smart card (إعداد بطاقة ذكية)، أدخل PIN وقم بتأكيده.
- لتغيير PIN الخاص بك—اكتب رقم PIN القديم ثم اختر رقمًا جديدًا.

استخدام لوحة معلومات Security Manager (إدارة الحماية)

لوحة معلومات Security Manager (إدارة الحماية) هي المكان الأساسي للوصول بسهولة إلى ميزات Security Manager (إدارة الحماية) وتطبيقاته وإعداداته.

تتكون لوحة المعلومات من المكونات التالية:

- **ID Card (بطاقة الهوية)**—تعرض اسم مستخدم Windows والصورة المحددة التي توضح حساب المستخدم الذي قام بتسجيل الدخول.
- **Security Applications (تطبيقات الحماية)**—تعرض قائمة موسعة بالارتباطات لتكوين فئات الحماية التالية:
  - **My Identity (هويتي)**
  - **My Data (بياناتي)**
  - **My Computer (جهاز الكمبيوتر)**
- **Discover more (اكتشف المزيد)**—يفتح صفحة يمكنك العثور فيها على تطبيقات إضافية لتعزيز حماية الهوية والبيانات والاتصالات الخصة بك.
- **Main area (الناحية الأساسية)**—تعرض الشاشات الخاصة بالتطبيق.
- **Administration (الإدارة)**—تفتح HP ProtectTools Administrative Console.

- زر **Help (التعليمات)**—يعرض معلومات حول الشاشة الحالية.
- **Advanced (متقدم)**—يسمح لك بالوصول إلى الخيارات التالية:
  - **Preferences (تفضيلات)**—تسمح لك بتخصيص إعدادات Security Manager (إدارة الحماية).
  - **Backup and Restore (النسخ الاحتياطي والاستعادة)**—يسمح لك بنسخ البيانات احتياطيًا واستعادتها.
  - **About (حول)**—يعرض معلومات الإصدار حول Security Manager (إدارة الحماية).

لفتح لوحة معلومات Security Manager (إدارة الحماية)، انقر فوق **Start (ابدأ)**، انقر فوق **All Programs (كافة البرامج)**, انقر فوق **HP**، ثم انقر فوق **HP ProtectTools Security Manager ((إدارة الحماية لـ HP ProtectTools)**.

فتح HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools)

يمكنك فتح HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) بأي من الطرق التالية:

- انقر فوق **Start (ابدأ)**، ثم **All Programs (كافة البرامج)**، ثم **HP**، ثم انقر فوق **HP ProtectTools Security Manager (إدارة الحماية لـHP ProtectTools)**.
- انقر نقراً مزدوجاً فوق الرمز **HP ProtectTools** في ناحية الإعلام أقصى يسار شريط المهام.
- انقر فوق الرمز **HP ProtectTools**، وانقر فوق **Open HP ProtectTools Security Manager (افتح إدارة الحماية لـ HP ProtectTools)**.
- انقر فوق أداة **Security Manager ID Card (بطاقة معرف Security Manager)** على شريط Windows الجانبي.
- اضغط مجموعة مفاتيح التشغيل السريع h+alt+ctrl لفتح قائمة Security Manager Quick Links (ارتباطات Security Manager السريعة).

المهام العامة

تساعدك التطبيقات المضمنة في هذه المجموعة على إدارة الجوانب المتنوعة لهويتك الرقمية.

- **Security Manager**(إدارة الحماية)—يقوم بإنشاء Quick Links (الارتباطات السريعة) وإدارتها، التي تسمح لك بتشغيل مواقع الويب والبرامج وتسجيل الدخول عليها عن طريق المصادقة باستخدام كلمة مرور Windows أو بصمات أصابعك أو بطاقة ذكية.
- **Credentials (بيانات الاعتماد)**—تقدم وسيلة لتغيير كلمة مرور Windows الخاصة بك بسهولة أو تسجيل بصمات أصابعك أو إعداد بطاقة ذكية.

لإضافة المزيد من التطبيقات، انقر فوق زر [+] **Discover more (اكتشف المزيد)** في الركن السفلي الأيمن من لوحة المعلومات. يمكن أن يقوم المسؤول بتعطيل هذا الزر.

Password Manager (إدارة كلمة مرور)

تسجيل الدخول على Windows ومواقع الويب والتطبيقات أسهل وأكثر آمنًا عند استخدام Password Manager (إدارة كلمة مرور). يمكنك استخدامه لإنشاء كلمات مرور أقوى بحيث لا تضطر إلى تدوينها أو تذكرها وتسجيل الدخول بعد ذلك بسهولة وسرعة بواسطة بصمة أصبع أو بطاقة ذكية أو كلمة مرور Windows الخاصة بك.

يقدم Password Manager (إدارة كلمة مرور) الخيارات التالية:

- إضافة مرات تسجيل الدخول أو تحريرها أو حذفها من علامة التبويب Manage (إدارة).
- استخدم Quick Links (الارتباطات السريعة) لتشغيل المستعرض الافتراضي وقم بتسجيل الدخول على أي موقع ويب أو برنامج بعد إعداده.
- قم بالسحب والإفلات لتنظيم Quick Links (الارتباطات السريعة) في فئات.
- انظر سريعًا ما إذا كانت أي من كلمات المرور الخاصة بك غير محمية وقم بإنشاء كلمة مرور معقدة وقوية تلقائيًا للاستخدام مع المواقع الجديدة.

العديد من ميزات Password Manager (إدارة كلمة مرور) متاحة أيضًا عبر رمز Password Manager (إدارة كلمة المرور) الذي يتم عرضه عند التركيز على شاشة تسجيل الدخول على صفحة الويب أو البرنامج. انقر فوق الرمز لعرض قائمة السياق التي يمكنك من خلالها الاختيار من بين الخيارات التالية.

لصفحات الويب أو البرامج التي لم يتم تسجيل الدخول عليها بعد

تظهر الخيارات التالية في قائمة السياق:

- **Add [somedomain.com] to the Password Manager (إضافة [somedomain.com] إلى Password Manager (إدارة كلمة مرور))**—يسمح لك بإضافة تسجيل الدخول على شاشة تسجيل الدخول الحالية.
- **Open Password Manager (فتح إدارة كلمة المرور)**—يقوم بتشغيل Password Manager (إدارة كلمة مرور).
- **Icon settings (إعدادات الرمز)**—يسمح لك بتحديد الحالات التي يتم فيها عرض رمز Password Manager (إدارة كلمة مرور).
- **Help (تعليمات)**—يعرض التعليمات الخاصة ببرنامج Password Manager (إدارة كلمة مرور).

لصفحات الويب أو البرامج التي تم تسجيل الدخول عليها بعد

تظهر الخيارات التالية في قائمة السياق:

- **Fill in logon data (ملء بيانات تسجيل الدخول)**—يضع بيانات تسجيل الدخول في حقول تسجيل الدخول ثم يرسل الصفحة (في حالة تحديد الإرسال عند إنشاء تسجيل الدخول أو تحريره في أخر مرة).
- **Edit logon (تحرير تسجيل الدخول)**—يسمح لك بتحرير بيانات تسجيل الدخول الخاصة بك على موقع الويب هذا.

- **Add a New Account (إضافة حساب جديد)**—يسمح لك بإضافة حساب لتسجيل الدخول.
- **Open Password Manager (فتح إدارة كلمة المرور)**—يقوم بتشغيل تطبيق Password Manager (إدارة كلمة مرور).
- **Help (تعليمات)**—يعرض التعليمات الخاصة ببرنامج Password Manager (إدارة كلمة مرور).

ملاحظة: قد يكون المسؤول عن هذا الكمبيوتر أعد Security Manager (إدارة الحماية) بحيث يطلب أكثر من بيان اعتماد واحد عند التحقق من هويتك.

إضافة تسجيلات الدخول

يمكنك إضافة تسجيل الدخول على موقع ويب أو برنامج بإدخال معلومات تسجيل الدخول مرة واحدة. منذ ذلك الحين سيبدأ Password Manager (إدارة كلمة مرور) بإدخال المعلومات الخاصة بك تلقائيًا. يمكنك استخدام تسجيلات الدخول تلك بعد الاستعراض وصولاً إلى موقع الويب أو البرنامج، أو النقر فوق تسجيل الدخول من قائمة **Logons (تسجيلات الدخول)** كي يقوم Password Manager (إدارة كلمة مرور) بفتح موقع الويب أو البرنامج وتسجيل دخولك عليه.

لإضافة تسجيل دخول:

١. افتح شاشة تسجيل الدخول لموقع الويب أو البرنامج

٢. انقر فوق السهم الموجود على رمز **Password Manager (إدارة كلمة المرور)**، ثم انقر على واحد مما يلي بناء على شاشة تسجيل الدخول وما إذا كانت لموقع ويب أم برنامج:

- لموقع ويب، انقر فوق **Add [domain name] to Password Manager (إضافة [اسم المجال] إلى Password Manager (إدارة كلمة مرور))**.
- لبرنامج، انقر فوق **Add this logon screen to Password Manager (إضافة شاشة تسجيل الدخول هذه إلى Password Manager (إدارة كلمة مرور))**.

٣. أدخل بيانات تسجيل الدخول. يتم تحديد حقول تسجيل الدخول على الشاشة، والحقول المناظرة لها على مربع الحوار بواسطة حد برتقالي عريض. يمكنك أيضًا عرض مربع الحوار هذا بالنقر فوق **Add Logon (إضافة تسجيل دخول)** من علامة التبويب **Password Manager (إدارة كلمة مرور)**. تعتمد بعض الخيارات على أجهزة الحماية المتصلة بالكمبيوتر؛ على سبيل المثال، استخدام مفتاح التشغيل السريع H+alt+ctrl أو مسح بصمة الأصبع الخاصة بك أو إدخال بطاقة ذكية.

- لملء حقل تسجيل دخول بإحدى الخيارات ذات التنسيق المسبق، انقر فوق الأسهم الموجودة إلى يسار الحقل.
- لإضافة حقول إضافية من الشاشة إلى تسجيل الدخول الخاص بك، انقر فوق **Choose other fields (اختر حقولاً أخرى)**.
- لملء حقول تسجيل الدخول دون إرسالها، قم بمسح خانة الاختيار **Submit logon data (إرسال بيانات تسجيل الدخول)**.
- لعرض كلمة المرور الخاصة بتسجيل الدخول هذا، انقر فوق **Show password (إظهار كلمة المرور)**.

٤. انقر فوق **OK (موافق)**.

تتم إزالة علامة الزائد من رمز Password Manager (إدارة كلمة المرور) لإعلامك بأنه تم إنشاء تسجيل الدخول.

في كل مرة تصل فيها إلى موقع الويب هذا أو تفتح هذا البرنامج، يتم عرض رمز Password Manager (إدارة كلمة المرور)، مشيرًا إلى إمكانية استخدامك لبيانات اعتمادك المسجلة في تسجيل الدخول.

تحرير تسجيلات الدخول

لتحرير تسجيل دخول، اتبع هذه الخطوات:

١. افتح شاشة تسجيل الدخول لموقع الويب أو البرنامج

٢. لعرض مربع حوار يمكنك فيه تحرير معلومات تسجيل الدخول الخاصة بك، انقر فوق السهم الموجود على رمز **Password Manager (إدارة كلمة المرور)**، ثم انقر فوق **Edit logon (تحرير تسجيل الدخول)**. يتم تحديد حقول تسجيل الدخول على الشاشة، والحقول المناظرة لها على مربع الحوار بواسطة حد برتقالي عريض.

يمكنك أيضًا عرض مربع الحوار هذا بالنقر فوق **Edit for the desired logon (تحرير لتسجيل الدخول المراد)** من علامة التبويب **Password Manager (إدارة كلمة مرور)**.

٣. حرر معلومات تسجيل الدخول.

- لملء حقل تسجيل دخول بإحدى الخيارات ذات التنسيق المسبق، انقر فوق الأسهم الموجودة إلى يسار الحقل.
- لإضافة حقول إضافية من الشاشة إلى تسجيل الدخول الخاص بك، انقر فوق **Choose other fields (اختر حقولاً أخرى)**.
- لملء حقول تسجيل الدخول دون إرسالها، قم بمسح خانة الاختيار **Submit logon data (إرسال بيانات تسجيل الدخول)**.
- لعرض كلمة المرور الخاصة بتسجيل الدخول هذا، انقر فوق **Show password (إظهار كلمة المرور)**.

٤. انقر فوق **OK (موافق)**.

استخدام قائمة تسجيلات الدخول

يقدم Password Manager (إدارة كلمة المرور) طرقة سريعة وسهلة لبدء تشغيل مواقع الويب والبرامج التي قمت بإنشاء تسجيلات دخول لها. انقر نقرًا مزدوجًا فوق تسجيل دخول برنامج أو موقع ويب من قائمة **Logons (تسجيلات الدخول)**، أو علامة التبويب **Manage (إدارة)** في **Password Manager (إدارة كلمة المرور)**، لفتح شاشة تسجيل دخول، ثم قم بملء بيانات تسجيل الدخول الخاصة بك.

عندما تنشأ تسجيل دخول، تتم إضافته تلقائيًا إلى قائمة Password Manager Logons (تسجيلات دخول Password Manager).

لعرض قائمة Logons (تسجيلات الدخول):

١. اضغط على مجموعة مفاتيح التشغيل السريع الخاصة بـ **Password Manager (إدارة كلمة المرور)**. h+alt+ctrl هي إعداد الشركة المصنعة. لتغيير مجموعة مفاتيح التشغيل السريع، انقر فوق **Password Manager (إدارة كلمة المرور)**، ثم انقر فوق **Settings (إعدادات)**.

٢. قم بمسح بصمة أصبعك (على أجهزة الكمبيوتر التي تحتوي على جهاز قراءة بصمات أصابع مدمج أو متصلة بجهاز من هذا النوع).

تنظيم تسجيلات الدخول إلى فئات

استخدم الفئات للاحتفاظ بتسجيلات الدخول الخاصة بك بشكل منظم بإنشاء فئة واحدة أو أكثر. ثم قم بسحب تسجيلات الدخول الخاصة بك وإفلاتها في الفئات المطلوبة.

لإضافة فئة:

١. من لوحة معلومات Security Manager (إدارة الحماية)، انقر فوق **Password Manager (إدارة كلمة المرور)**.

٢. انقر فوق علامة التبويب **Manage (إدارة)**، ثم انقر فوق **Add Category (إضافة فئة)**

٣. أدخل اسم للفئة.

٤. انقر فوق **OK (موافق)**.

لإضافة تسجيل دخول إلى فئة:

١. ضع مؤشر الماوس على تسجيل الدخول المطلوب.

٢. اضغط على زر الماوس الأيسر باستمرار.

٣. اسحب تسجيل الدخول إلى قائمة الفئات. سيتم تمييز الفئات عنهد تمرير الماوس أعلاهم.

٤. قم بإفلات زر الماوس عندما يتم تمييز الفئة المرادة.

لن يتم نقل تسجيلات الدخول إلى الفئة، حيث سيتم نسخها فقط إلى الفئة المحددة. يمكنك إضافة تسجيل الدخول ذاته إلى أكثر من فئة، ويمكنك عرض كل تسجيلات الدخول الخاصة بك بالنقر فوق **All (كل)**.

إدارة تسجيلات الدخول الخاصة بك

يسهل Password Manager (إدارة كلمة المرور) إدارة معلومات تسجيل الدخول بالنسبة لأسماء المستخدمين وكلمات المرور وحسابات تسجيل الدخول المتعددة من مكان واحد مركزي.

تسجيلات الدخول الخاصة بك مدرجة في علامة التبويب Manage (إدارة). إذا تم إنشاء تسجيلات دخول متعددة لنفس موقع الويب، يتم إدراج كل تسجيل دخول تحت اسم موقع الويب ووضع مسافة قبله في قائمة تسجيلات الدخول.

لإدارة تسجيلات الدخول الخاصة بك:

من لوحة معلومات Security Manager (إدارة الحماية)، انقر فوق **Password Manager (إدارة كلمة المرور)**، ثم انقر فوق علامة التبويب **Manage (إدارة)**.

- **إضافة تسجيل دخول**—انقر فوق **Add Logon (إضافة تسجيل دخول)** ثم اتبع الإرشادات التي تظهر على الشاشة.
- **تحرير تسجيل دخول**—انقر فوق تسجيل دخول، انقر فوق **Edit (تحرير)**، ثم قم بتغيير بيانات تسجيل الدخول.
- **حذف تسجيل دخول**—انقر فوق تسجيل دخول ثم انقر فوق **Delete (حذف)**.

لإضافة تسجيل دخول إضافي لموقع ويب أو برنامج:

١. افتح شاشة تسجيل الدخول لموقع الويب أو البرنامج

٢. انقر فوق رمز **Password Manager (إدارة كلمة مرور)** لعرض قائمته المختصرة.

٣. انقر فوق **Add additional logon (إضافة تسجيل دخول إضافي)**، ثم اتبع الإرشادات التي تظهر على الشاشة.

تقييم قوة كلمة المرور الخاصة بك

استخدام كلمات مرور قوية لتسجيل الدخول على مواقع الويب أو البرامج الخاصة بك من الأمور الهامة لحماية هويتك.

يسهل Password Manager (إدارة كلمة مرور) مراقبة مستوى حمايتك وتحسينه عن طريق التحليل الفوري والتلقائي لقوة كل كلمة مرور يتم استخدامها لتسجيل الدخول على مواقع الويب والبرامج الخاصة بك.

إعدادات رمز Password Manager (إدارة كلمة مرور)

يحاول Password Manager (إدارة كلمة مرور) التعرف على شاشات تسجيل الدخول على مواقع الويب والبرامج. وعند اكتشافه لشاشة تسجيل دخول لم تقم بإنشاء تسجيل دخول لها، يطالبك Password Manager (إدارة كلمة مرور) بإضافة تسجيل دخول للشاشة بعرض رمز Password Manager (إدارة كلمة مرور) مصحوبًا بعلامة "+".

اضغط فوق سهم الرمز، ثم انقر فوق **Icon Settings (إعدادات الرمز)** لتخصيص كيفية تعامل **Password Manager (إدارة كلمة مرور)** مع مواقع تسجيل الدخول المحتمل.

- **Prompt to add logons for logon screens (مطالبة بإضافة تسجيلات دخول لشاشات تسجيل الدخول)**—انقر فوق هذا الخيار كي يطالبك Password Manager (إدارة كلمة مرور) بإضافة تسجيل دخول عند عرض شاشة تسجيل دخول التي لم يتم إعداد تسجيل دخول لها بالفعل.
- **Exclude this screen (استبعاد هذه الشاشة)**—حدد خانة الاختيار بحيث لا يطالبك Password Manager (إدارة كلمة مرور) مجددًا بإضافة تسجيل دخول إلى شاشة تسجيل الدخول هذه.

للوصول إلى إعدادات Password Manager (إدارة كلمة مرور) الإضافية، انقر فوق **Password Manager (إدارة كلمة مرور)**، ثم انقر فوق **Settings (إعدادات)** على لوحة معلومات Security Manager (إدارة الحماية).

إعدادات

يمكنك تحديد إعدادات لتخصيص HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools):

١. **Prompt to add logons for logon screens (مطالبة بإضافة تسجيلات دخول لشاشات تسجيل الدخول)**—يتم عرض رمز Password Manager (إدارة كلمة مرور) مصحوبًا بعلامة زائد في كل مرة يتم فيها اكتشاف شاشة تسجيل دخول على موقع ويب أو برنامج، وهو ما يشير إلى إمكانية إضافتك تسجيل دخول لهذه الشاشة إلى الوسيلة الداعمة لكلمة المرور. لتعطيل هذه الميزة، في مربع الحوار **Icon Settings (إعدادات الرمز)**، امسح خانة الاختيار الموجودة بجوار **Prompt to add logons for logon screens (مطالبة بإضافة تسجيلات دخول لشاشات تسجيل الدخول)**.

٢. **Open Password Manager with H+alt+ctrl (فتح Password Manager (إدارة كلمة مرور) بواسطة H+alt+ctrl)**—مفتاح التشغيل السريع الافتراضي الذي يفتح قائمة Manager Quick Links (الارتباطات السريعة لإدارة كلمة المرور) هو H+alt+ctrl. لتغيير مفتاح التشغيل السريع، انقر فوق هذا الخيار وأدخل مجموعة جديدة من المفاتيح. قد تتضمن المجموعات واحدة أو أكثر مما يلي: shift or alt, ctrl، وأي مفتاح أبجدي أو رقمي.

٣. انقر فوق **Apply (تطبيق)** لعرض التغييرات.

بيانات الاعتماد

تستخدم بيانات اعتماد Security Manager (إدارة الحماية) الخاصة بك لتأكيد هويتك. يمكن للمسؤول المحلي عن هذا الكمبيوتر إعداد أي من البيانات سيتم استخدامها لإثبات هويتك عند الدخول على حساب Windows أو مواقع الويب أو البرامج الخاصة بك.

يمكن أن تتغير بيانات الاعتماد المتاحة تبعًا لأجهزة الحماية المدمجة في هذا الكمبيوتر أو المتصلة به. سيكون لكل بيان اعتماد مدعم إدخال في المجموعة **My Identity, Credentials (هويتي، بيانات الاعتماد)**.

بيانات الاعتماد والمتطلبات والحالة الحالية مدرجة وقد تتضمن ما يلي:

- بصمات الأصابع
- كلمة المرور
- البطاقة الذكية Smart card

لتسجيل بيان اعتماد أو تغييره، انقر فوق الارتباط واتبع الإرشادات التي تظهر على الشاشة.

بطاقة المعرف الشخصي الخاص بك

تشير بطاقة المعرف الخاصة بك على نحو فريد إلى كونك مالك حساب Windows هذا، حيث يعرض اسمك والصورة التي تختارها. وتظل معروضة بشكل دائم في الركن العلوي الأيمن لصفحات Security Manager (إدارة الحماية)، وكأداة على شريط Windows الجانبي.

يعد النقر فوق بطاقة المعرف الخاصة بك في شريط Windows الجانبي طريقة من طرق متعددة للوصول إلى Security Manager (إدارة الحماية).

يمكنك تغيير الصورة وطريقة عرض اسمك. افتراضيًا، يتم إظهار اسم مستخدم Windows الكامل والصورة التي تختارها أثناء إعداد Windows.

لتغيير الاسم المعروض:

١. من لوحة معلومات Security Manager (إدارة الحماية)، انقر فوق **ID Card (بطاقة المعرف)** في الركن الأيمن العلوي.

٢. انقر فوق المربع الذي يعرض الاسم الذي أدخلته لحساب Windows الخاص بك. سيعرض النظام اسم مستخدم Windows الخاص بك لهذا الحساب.

٣. لتغيير هذا الاسم، اكتب الاسم الجديد، ثم انقر فوق الزر **Save (حفظ)**.

لتغيير الصورة المعروضة:

١. من لوحة معلومات Security Manager (إدارة الحماية)، انقر فوق **My Identity (هويتي)** ثم انقر فوق **ID Card (بطاقة المعرف)** في الركن الأيمن العلوي.

٢. انقر فوق الزر **Choose picture (اختر صورة)**، انقر فوق صورة، ثم انقر فوق الزر **Save (حفظ)**.

إعداد التفضيلات الخاصة بك

يمكنك تخصيص إعدادات HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools). من لوحة معلومات Security Manager (إدارة الحماية)، انقر فوق **Advanced (متقدم)**، ثم انقر فوق **Preferences (تفضيلات)**. يتم عرض الإعدادات المطلوبة في علامتي تبويب: العامة وبصمة الأصبع.

General (عام)

الإعدادات التالية متاحة في علامة التبويب العامة:

Appearance (ظهور)—تظهر الرمز على شريط المهام

لتمكين عرض الرمز على شريط المهام، حدد خانة الاختيار.

لتعطيل عرض الرمز على شريط المهام، امسح خانة الاختيار.

Fingerprint (بصمة الأصبع)

الإعدادات التالية متاحة في علامة التبويب بصمة الأصبع:

Quick Actions (الإجراءات السريعة)—استخدم Quick Actions (الإجراءات السريعة) لتحديد مهمة Security Manager (إدارة الحماية) التي سيتم القيام بها عند الضغط على زر معين لأسفل في الوقت الذي يتم فيه مسح بصمة الأصبع.

لتعيين إجراء سريع لواحد من المفاتيح المسردة:

- انقر فوق الخيار **Fingerprint+(Key) (المفتاح + بصمة الأصبع)**، ثم انقر فوق واحدة من المهام المتاحة من القائمة.

Fingerprint Scan Feedback (ملاحظات مسح بصمة الأصبع)—يظهر فقط عندما يكون هناك جهاز قراءة بصمات أصابع متاحًا. استخدم هذا الإعداد للتعامل مع الملاحظات التي ظهرت عند مسحك لبصمة أصبعك.

- **Enable sound feedback (تمكين الملاحظات الصوتية)**—يقدم Security Manager (إدارة الحماية) لك ملاحظات صوتية عند مسح بصمة الأصبع، ويقوم بتشغيل أصوات مختلفة لأحداث البرنامج المعينة. يمكنك تخصيص أصوات جديدة لهذه الأحداث عن طريق علامات التبويب Sounds (أصوات) في لوحة تحكم Windows أو تعطيل الملاحظات الصوتية عند مسح هذا الخيار.
- **Show scan quality feedback (إظهار ملاحظات جودة المسح)**—افتراضيًا، يظهر Security Manager (إدارة الحماية) صورة لبصمة أصبع مصحوبة بعلامة استفهام حينما تكون جودة مسح بصمة الأصبع غير كافية لمصادقتك. يمكنك تعطيل عرض هذه الصورة بمسح هذا الخيار.

نسخ بياناتك احتياطيًا واستعادتها

يوصى بنسخ بيانات Security Manager (إدارة الحماية) احتياطيًا الخاصة بك بشكل منتظم. يتوقف عدد مرات النسخ الاحتياطي على معدل التغييرات التي تلحق بالبيانات. على سبيل المثال، إذا قمت بإضافة تسجيلات الدخول يوميًا، يتعين عليك نسخ بياناتك احتياطيًا بشكل يومي.

يمكن استخدام النسخ الاحتياطية لترحيل البيانات من كمبيوتر إلى أخر، وهو ما يعرف أيضًا بالاستيراد والتصدير.

ملاحظة: يتم نسخ البيانات احتياطيًا فقط وفقًا لهذه الميزة.

يجب تثبيت برنامج HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) على أي كمبيوتر لتلقي البيانات المنسوخة احتياطيًا قبل التمكن من استعادة البيانات من ملف النسخ الاحتياطي.

لنسخ بياناتك احتياطيًا:

١. في اللوحة اليمنى انقر فوق **Advanced (متقدم)**، ثم انقر فوق **Backup and Restore (نسخ احتياطي واستعادة)**.

٢. انقر فوق **Back up computer (النسخ الاحتياطي للبيانات)**.

٣. حدد الوحدات التي ترغب في تضمينها في النسخ الاحتياطي. في معظم الحالات، سترغب في تحديد الوحدات كافة.

٤. أدخل اسم لملف التخزين. افتراضيًا، سيتم حفظ الملف في مجلد المستندات. انقر فوق **Browse (استعراض)** لتحديد مكان مختلف.

٥. أدخل كلمة مرور لحماية الملف.

٦. أكد هويتك.

٧. انقر فوق **Finish (إنهاء)**.

لاستعادة بياناتك:

١. في اللوحة اليمنى انقر فوق **Advanced (متقدم)**،ثم انقر فوق **Backup and Restore (نسخ احتياطي واستعادة)**.

٢. انقر فوق **Restore files (استعادة الملفات)**.

٣. حدد ملف التخزين الذي تم إنشاؤه مسبقًا. يمكنك إدخال المسار في الحقل المقدم، أو انقر فوق **Edit (تحرير)**.

٤. أدخل كلمة المرور المستخدمة في حماية الملف.

٥. حدد الوحدات التي ترغب في استعادة بياناتها. في معظم الحالات، ستكون كل الوحدات المدرجة.

٦. انقر فوق **Finish (إنهاء)**.

إضافة تطبيقات

قد تكون هناك تطبيقات إضافية تقدم ميزات جديدة لهذا البرنامج.

من لوحة معلومات Security Manager (إدارة الحماية)، انقر فوق **Discover more [+] (اكتشف المزيد [+])** لاستعراض التطبيقات الإضافية.

ملاحظة: إذا لم يظهر الارتباط **Discover more [+] (اكتشف المزيد [+])** في الجزء السفلي الأيمن من لوحة المعلومات، يكون المسؤول عن هذا الكمبيوتر قد قام بتعطيلها.

حالة تطبيقات الحماية

تعرض صفحة حالة تطبيقات Security Manager (إدارة الحماية) الحالة الإجمالية لتطبيقات الحماية المثبتة. حيث تعرض التطبيقات المثبتة وحالة التثبيت الخاصة بكل تطبيق. يتم عرض الملخص تلقائيًا عندما تفتح لوحة معلومات Security Manager (إدارة الحماية) أو عندما تنقر فوق **Security Applications (تطبيقات الحماية)**.

٧ Drive Encryption for HP ProtectTools (تشفير محركات الأقراص لـ HP ProtectTools) (طرز مختارة فقط)

△ **تنبيه:** إذا قررت إلغاء تثبيت الوحدة النمطية Drive Encryption (تشفير محركات الأقراص), وجب حل شفرة كافة محركات الأقراص المشفرة أولا. وإلا, فلا يمكنك الوصول إلى البيانات الموجودة في محركات الأقراص المشفرة إلا إذا سجلت في خدمة الاستعادة الخاصة بـDrive Encryption (تشفير محركات الأقراص). لا تتيح لك إعادة تثبيت الوحدة النمطية Drive Encryption (تشفير محركات الأقراص) الوصول إلى محركات الأقراص المشفرة.

يعمل Drive Encryption (تشفير محركات الأقراص) لـ HP ProtectTools على إكمال حماية البيانات بتشفير القرص الصلب الخاص بالكمبيوتر. عند تنشيط Drive Encryption (تشفير محركات الأقراص)، ينبغي عليك الدخول في شاشة تسجيل الدخول الخاصة بـ Drive Encryptio، والتي يتم عرضها قبل بدء نظام تشغيل Windows®.

يسمح HP ProtectTools Setup Wizard (معالج الإعداد لـ HP ProtectTools) لمسؤولي Windows بتنشيط Drive Encryption (تشفير محركات الأقراص) راجع تعليمات برنامج HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) للحصول على المزيد من المعلومات.

يمكن القيام بالمهام التالية مع Drive Encryption (تشفير محركات الأقراص):

- إدارة التشفير
  - تشفير الأقراص الصلبة المفردة أو فك تشفيرها

ملاحظة: يمكن تشفير الأقراص الصلبة الداخلية فقط.

- الاستعادة
  - إنشاء نسخ احتياطية من المفاتيح
  - إجراء استعادة

إجراءات الإعداد

فتح Drive Encryption (تشفير محركات الأقراص)

١. انقر فوق **Start (ابدأ)**، ثم **All Programs (كافة البرامج)**، ثم **HP**، ثم انقر فوق **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**.

٢. في الجزء الأيمن، انقر فوق **Device Manager (إدارة الأجهزة)**.

المهام العامة

تنشيط Drive Encryption (تشفير محركات الأقراص)

استخدم HP ProtectTools Setup Wizard (معالج الإعداد لـ HP ProtectTools) لتنشيط Drive Encryption (تشفير محركات الأقراص).

ملاحظة: يستخدم هذا المعالج أيضًا في إضافة المستخدمين وحذفهم.

– أو –

١. انقر فوق **Start (ابدأ)**، ثم **All Programs (كافة البرامج)**، ثم **HP**، ثم انقر فوق **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**.

٢. في القائمة Tools (أدوات)، انقر فوق **Security (حماية)**، وانقر فوق **Features (ميزات)**.

٣. حدد خانة الاختيار **Drive Encryption (تشفير محركات الأقراص)**، ثم انقر فوق **Next (التالي)**.

٤. تحت **Drives to be encrypted (الأقراص الصلبة التي ستم تشفيرها)**، حدد خانة الاختيار للقرص الصلب الذي ترغب في تشفيره.

٥. أدخل جهاز التخزين في الفتحة المناسبة.

ملاحظة: لحفظ مفتاح التشفير، يجب أن تستخدم جهاز تخزين USB بتنسيق FAT32.

٦. تحت **External storage device on which to save encryption key (جهاز التخزين الخارجي الذي سيتم حفظ مفتاح التشفير عليه)**، حدد خانة الاختيار لجهاز التخزين الذي سيتم حفظ مفتاح التشفير عليه.

٧. انقر فوق **Apply (تطبيق)**.

يبدأ Drive Encryption (تشفير محركات الأقراص) في العمل.

راجع تعليمات برنامج HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) للحصول على المزيد من المعلومات.

إلغاء تنشيط Drive Encryption (تشفير محركات الأقراص)

استخدم HP ProtectTools Setup Wizard (معالج الإعداد لـ HP ProtectTools) لإلغاء تنشيط Drive Encryption (تشفير محركات الأقراص). راجع تعليمات برنامج HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) للحصول على المزيد من المعلومات.

– أو –

١. انقر فوق **Start (ابدأ)**، ثم **All Programs (كافة البرامج)**، ثم **HP**، ثم انقر فوق **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**.

٢. في القائمة Tools (أدوات)، انقر فوق **Security (حماية)**، وانقر فوق **Features (ميزات)**.

٣. حدد خانة الاختيار **Drive Encryption (تشفير محركات الأقراص)**، ثم انقر فوق **Apply (تطبيق)**.

يبدأ Drive decryption في العمل.

تسجيل الدخول بعد تنشيط Drive Encryption (تشفير محركات الأقراص)

عند تشغيلك للكمبيوتر بعد تنشيط Drive Encryption (تشفير محركات الأقراص) وتسجيل حصاب المستخدم الخاص بك، ينبغي عليك الدخول في شاشة تسجيل دخول Drive Encryption (تشفير محركات الأقراص):

ملاحظة: إذا قام مسؤول Windows بتمكين Pre-boot Security (الحماية ما قبل التمهيد) في HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools)، ستدخل على الكمبيوتر مباشرة بعد تشغيل الكمبيوتر، بدلاً من شاشة تسجيل دخول Drive Encryption (تشفير محركات الأقراص).

١. انقر فوق اسم المستخدم، ثم اكتب كلمة مرور Windows أو رقم Java™ Card PIN أو اضغط أصبع مسجل.

٢. انقر فوق **OK (موافق)**.

ملاحظة: إذا استخدمت مفتاح استعادة لدخول شاشة تسجيل دخول Drive Encryption (تشفير محركات الأقراص)، فستتم مطالبتك بتحديد اسم مستخدم Windows وكتابة كلمة المرور الخاصة بك في شاشة تسجيل دخول Windows.

حماية البيانات بتشفير القرص الصلب الخاص بك

استخدم HP ProtectTools Setup Wizard (معالج الإعداد لـ HP ProtectTools) لحماية البيانات بتشفير القرص الصلب:

١. في Security Manager (إدارة الحماية)، انقر فوق **Getting Started (الشروع في العمل)**، ثم انقر فوق رمز **Security Manager Setup (إعداد Security Manager)**. سيبدأ عرض يصف ميزات Security Manager (إدارة الحماية). (يمكنك أيضًا بدء تشغيل Security Manager (إدارة الحماية) من صفحة "Drive Encryption" (تشفير محركات الأقراص).)

٢. في الجزء الأيمن، انقر فوق **Drive Encryption (تشفير محركات الأقراص)**، ثم انقر فوق **Encryption Management (إدارة التشفير)**.

٣. انقر فوق **Change Encryption (تغيير التشفير)**.

٤. حدد القرص الصلب أو الأقراص الصلبة التي سيتم تشفيرها.

ملاحظة: يوصى بشدة بتشفير القرص الصلب.

عرض حالة التشفير

يمكن للمستخدمين عرض حالة التشفير من خلال HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools).

ملاحظة: يجب إجراء التغييرات الخاصة بحالة تشفير القرص الصلب باستخدام HP ProtectTools Administrative Console (وحدة تحكم إدارية لـ HP ProtectTools).

١. افتح **HP ProtectTools Security Manager** (إدارة الحماية لـ HP ProtectTools).

٢. تحت **My Data (بياناتي)**، انقر فوق **Encryption Status (حالة التشفير)**.

إذا كان Drive Encryption (تشفير محركات الأقراص) نشطًا، سيعرض القرص الصلب أحد أكواد الحالة التالية:

- نشط
- غير نشط
- غير مشفر
- مشفر
- تشفير
- فك تشفير

إذا كان القرص الصلب في عملية التشفير أو فك التشفير، فسيعرض شريط التقدم النسبة المكتملة والوقت المتبقي لإكمال التشفير أو فك التشفير.

المهام المتقدمة

إدارة Drive Encryption (تشفير محركات الأقراص) (مهمة للمسؤولين)

تسمح الصفحة Encryption Management (دارة التشفير) للمسؤولين بعرض حالة Drive Encryption (تشفير محركات الأقراص) وتغييرها (نشط أو غير نشط) وبعرض حالة التشفير الخاصة بكل الأقراص الصلبة على الكمبيوتر.

- إذا كانت الحالة غير نشطة، فأن ذلك يشير إلى عدم تنشيط Drive Encryption (تشفير محركات الأقراص) بعد في HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools) بواسطة مسؤول Windows وعدم حمايته للقرص الصلب. استخدم HP ProtectTools Security Manager Setup Wizard (معالج الإعداد الخاص بإدارة الحماية لـ HP ProtectTools) لتنشيط Drive Encryption.
- إذا كانت الحالة نشط، فأن ذلك يشير إلى أن Drive Encryption (تشفير محركات الأقراص) منشط ومكون. القرص الصلب في إحدى الحالات التالية:
  - غير مشفر
  - مشفر
  - تشفير
  - فك تشفير

تشفير الأقراص الصلبة المفردة أو فك تشفيرها

لتشفير قرص صلب واحد أو أكثر على الكمبيوتر أو إلغاء تشفير قرص تم تشفيره بالفعل، استخدم ميزة Change Encryption:

١. افتح **HP ProtectTools Administrative Console (وحدة تحكم إدارية لـ HP ProtectTools)**، انقر فوق **Drive Encryption (تشفير محركات الأقراص)**، ثم انقر فوق **Encryption Management (إدارة الشفير)**.

٢. انقر فوق **Change Encryption (تغيير التشفير)**.

٣. في مربع الحوار Change Encryption (تغيير التشفير)، حدد أو امسح خانة الاختيار المجاورة لكل قرص صلب ترغب في تشفيره أو إلغاء تشفيره، ثم انقر فوق **OK (موافق)**.

ملاحظة: عند تشفير القرص الصلب أو إلغاء تشفيره، فسيعرض شريط التقدم الوقت المتبقي لإكمال العملية أثناء الجلسة الحالية. إذا تم إيقاف تشغيل الكمبيوتر أو دخوله وضعَ Sleep (السكون) أو Hibernation (الإسبات) خلال إجراء التشفير ثم إعادة تشغيله يعاد ضبط عرض Time Remaining (الوقت المتبقي) على ما كان عليه في البداية، ولكنه يستمر التشفير الفعلي بداية من النقطة التي توقف عندها. سيتغير عرض الوقت المتبقي والتقدم بسرعة أكبر كي يعكس التقدم السابق

النسخ الاحتياطي والاستعادة (مهمة للمسؤولين)

تسمح صفحة Recovery (الاستعادة) للمسؤولين بعمل نسخ احتياطية من المفاتيح واستعادتها.

Local Drive Encryption Key Backup (نسخ مفتاح التشفير لمحرك الأقراص المحلي احتياطيًا)—يسمح لك بعمل نسخة احتياطية من مفاتيح التشفير على الوسائط القابلة للإزالة عند تنشيط Drive Encryption (تشفير محركات الأقراص).

إنشاء نسخ احتياطية من المفاتيح

يمكنك عمل نسخة احتياطية من مفتاح التشفير للقرص الصلب المشفر على جهاز تخزين قابل للإزالة:

△ **تنبيه:** تأكد من أن جهاز التخزين الذي يحتوي على النسخة الاحتياطية من المفتاح موجود بمكان آمن، لأنك إذا فقدت كلمة المرور أو بطاقة Java الخاصة بك، لن يمكنك الوصول إلى القرص الصلب الخاص بك سوى عن طريق هذا الجهاز.

١. افتح **HP ProtectTools Administrative Console (وحدة تحكم إدارية لـ HP ProtectTools)**، انقر فوق **Drive Encryption (تشفير محركات الأقراص)**، ثم انقر فوق **Recovery (استعادة)**.

٢. انقر فوق **Backup Keys (نسخ المفاتيح الاحتياطية)**.

٣. في صفحة Select Backup Disk (تحديد قرص النسخة الاحتياطية)، حدد خانة الاختيار للجهاز الذي ترغب في وضع نسخة المفتاح الاحتياطية عليه، ثم انقر فوق **Next (التالي)**.

٤. اقرأ المعلومات الموجودة في الصفحة التالية المعروضة، ثم انقر فوق **Next (التالي)**. يتم حفظ مفتاح التشفير على جهاز التخزين الذي تحدده.

٥. عند فتح مربع حوار التأكيد، انقر فوق **Finish (إنهاء)**.

إجراء استعادة

لإجراء الاستعادة في حالة نسيان كلمة المرور، اتبع هذه الخطوات:

١. قم بتشغيل الكمبيوتر.

٢. أدخل جهاز التخزين القابل للإزالة والذي يحتوي على نسخة المفتاح الاحتياطية.

٣. عند فتح مربع الحوار الخاص بتسجيل الدخول على Drive Encryption (تشفير محركات الأقراص) لـ HP ProtectTools، انقر فوق **Cancel (إلغاء الأمر)**.

٤. انقر فوق **Options (خيارات)** في الركن الأيمن السفلي من الشاشة، ثم انقر فوق **Recovery (استعادة)**.

٥. حدد الملف الذي يحتوي على النسخة الاحتياطية من المفتاح أو انقر فوق **Browse (استعراض)** للبحث عنه، ثم انقر فوق **Next (التالي)**.

٦. عند فتح مربع حوار التأكيد، انقر فوق **OK (موافق)**.

يبدأ الكمبيوتر الخاص بك.

ملاحظة: يوصى بإعادة تعيين كلمة المرور الخاصة بك بعد إجراء الاستعادة.

٨ Privacy Manager (إدارة الخصوصية) لـHP ProtectTools (طرز مختارة فقط)

تمكنك Privacy Manager for HP ProtectTools (إدارة الخصوصية لـHP ProtectTools) من استخدام وسائل متقدمة لتسجيل الدخول الآمن (المصادقة) للتحقق من المصدر والتكامل والأمن الخاص بالاتصال عند استخدام البريد الإلكتروني، أو مستندات Microsoft® Office أو الرسائل الفورية (IM).

تعزز Privacy Manager (إدارة الخصوصية) من البنية التحتية الخاصة بالأمن والتي يوفرها HP ProtectTools Security Manager (إدارة الحماية لـHP ProtectTools) الذي يشتمل على وسائل تسجيل الدخول الآمن التالية:

- المصادقة بواسطة بصمة الإصبع
- كلمة مرور Windows®
- بطاقة HP ProtectTools Java™ Card

يمكنك استخدام أي من أساليب تسجيل الدخول الآمن السابقة في Privacy Manager (إدارة الخصوصية).

تتطلب Privacy Manager (إدارة الخصوصية) ما يلي:

- HP ProtectTools Security Manager 5.00 (إدارة الحماية لـHP ProtectTools) الإصدار 5.00 أو أعلى
- أنظمة تشغيل Windows® 7 أو Windows Vista® أو Windows XP
- Microsoft Outlook 2007 أو Microsoft Outlook 2003
- حساب بريد إلكتروني صالح

ملاحظة: يجب طلب Privacy Manager Certificate (شهادة إدارة الخصوصية (شهادة رقمية)) وتثبيتها من داخل Privacy Manager (إدارة الخصوصية) كي تتمكن من الوصول إلى ميزات الأمن. للحصول على المعلومات بشأن طلب Privacy Manager Certificate (شهادة إدارة الخصوصية)، راجع طلب Privacy Manager Certificate (شهادة إدارة الخصوصية) وتثبيتها في صفحة ٤٢.

إجراءات الإعداد

فتح Privacy Manager (إدارة الخصوصية)

لفتح Privacy Manager (إدارة الخصوصية)

١. انقر فوق **Start (ابدأ)**، ثم **All Programs (كافة البرامج)**، ثم **HP**، ثم انقر فوق **HP ProtectTools Security Manager (إدارة الحماية لـHP ProtectTools)**.

٢. انقر فوق **Privacy Manager** (إدارة الخصوصية).

– أو –

انقر بزر الماوس الأيمن فوق رمز **HP ProtectTools** الموجود في ناحية الإعلام، أقصى يمين شريط المهام، ثم انقر فوق **Privacy Manager** (إدارة الخصوصية) ثم فوق **Configuration** (تكوين).

– أو –

في شريط المهام الموجود بأي من رسائل البريد الإلكتروني في Microsoft Outlook، انقر فوق السهم إلى الأسفل الموجود بجوار **Send Securely (الإرسال الآمن)**، ثم انقر فوق **Certificates (الشهادات)** أو **Trusted Contacts (جهات الاتصال الموثوق بها)**.

– أو –

في شريط المهام الموجود بأي من مستندات Microsoft Office، انقر فوق السهم إلى الأسفل الموجود بجوار **Sign and Encrypt (التوقيع والتشفير)**، ثم انقر فوق **Certificates (الشهادات)** أو **Trusted Contacts (جهات الاتصال الموثوق بها)**.

إدارة Privacy Manager Certificates (شهادات إدارة الخصوصية)

تقوم Privacy Manager certificates (شهادات إدارة الخصوصية) بحماية البيانات والرسائل بواسطة تقنية تشفير تسمى البنية التحتية العامة للمفاتيح (PKI). تتطلب PKI حصول المستخدمين على مفاتيح تشفير و Privacy Manager Certificate (شهادة إدارة الخصوصية) تصدرها إحدى السلطات الخاصة بالشهادات (CA) بخلاف معظم برامج تشفير البيانات والمصادقة عليها التي تتطلب منك المصادقة بصورة دورية فقط، فإن Privacy Manager (إدارة الخصوصية) تتطلب المصادقة في كل مرة تقوم فيها بالتوقيع على رسالة بريد إلكترونية أو إحدى مستندات Microsoft Office بواسطة مفتاح تشفير. تعمل Privacy Manager (إدارة الخصوصية) على جعل عملية حفظ المعلومات الهامة وإرسالها آمنة.

يمكن إجراء المهام التالية:

- طلب Privacy Manager Certificate (شهادة إدارة الخصوصية) وتثبيتها
- عرض تفاصيل Privacy Manager Certificate (شهادة إدارة الخصوصية)
- تجديد Privacy Manager Certificates (شهادات إدارة الخصوصية)
- في حالة توفر عدة شهادات، قم بتحديد Privacy Manager Certificate (شهادة إدارة الخصوصية) افتراضية كي تستخدمها Privacy Manager (إدارة الخصوصية)
- حذف Privacy Manager Certificate (شهادة إدارة الخصوصية) وإلغاءها (متقدم)

طلب Privacy Manager Certificate (شهادة إدارة الخصوصية) وتثبيتها

كي تتمكن من استخدام ميزات Privacy Manager (إدارة الخصوصية)، يجب عليك طلب Privacy Manager Certificate (شهادة إدارة الخصوصية (من داخل Privacy Manager (إدارة الخصوصية))) وتثبيتها مستخدمًا عنوان بريد إلكتروني صالح. يجب إعداد عنوان البريد الإلكتروني كحساب في Microsoft Outlook على نفس الكمبيوتر الذي تستخدمه في طلب Privacy Manager Certificate (شهادة إدارة الخصوصية).

طلب Privacy Manager Certificate (شهادة إدارة الخصوصية)

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Certificates (الشهادات)**.

٢. انقر فوق **طلب Privacy Manager Certificate (شهادة إدارة الخصوصية)**.

٣. في صفحة "Welcome" ("مرحبًا")، قم بقراءة النص ثم انقر فوق **Next (التالي)**.

٤. في صفحة "License Agreement" ("اتفاقية الترخيص")، قم بقراءة اتفاقية الترخيص.

٥. تأكد من أنه قد تم تحديد خانة الاختيار الموجودة بجوار **Check here to accept the terms of this license agreement (حدد هنا لقبول شروط اتفاقية الترخيص هذه)**، ثم انقر فوق **Next (التالي)**.

٦. في صفحة "Your Certificate Details" ("تفاصيل الشهادة الخاصة بك")، أدخل البيانات المطلوبة ثم انقر فوق **Next (التالي)**.

٧. في صفحة "Certificate Request Accepted" ("تم قبول طلب الشهادة")، انقر فوق **Finish (إنهاء)**.

٨. انقر فوق **OK (موافق)** لإغلاق الشهادة.

سوف تستلم بريد إلكتروني في Microsoft Outlook مرفق به Privacy Manager Certificate (شهادة إدارة الخصوصية) الخاصة بك.

الحصول على Privacy Manager Corporate Certificate (شهادة إدارة الخصوصية الخاصة بالشركات) معينة مسبقًا

١. في Outlook، قم بفتح البريد الإلكتروني الذي استلمته والذي يبين أنه قد تم تعيين شهادة خاصة بالشركات مسبقًا إليك.

٢. انقر فوق **Obtain (الحصول على)**.

٣. سوف تستلم بريد إلكتروني في Microsoft Outlook مرفق به Privacy Manager Certificate (شهادة إدارة الخصوصية) الخاصة بك.

٤. لتثبيت الشهادة، راجع تثبيت Privacy Manager Certificate (شهادة إدارة الخصوصية) في صفحة ٤٣

تثبيت Privacy Manager Certificate (شهادة إدارة الخصوصية)

١. عندما تستلم البريد الإلكتروني المرفق به Privacy Manager Certificate (شهادة إدارة الخصوصية) الخاصة بك، قم بفتح البريد الإلكتروني ثم انقر فوق زر **Setup (إعداد)** الموجود في الزاوية السفلى اليمنى من الرسالة في Outlook 2007، أو في الزاوية العليا اليسرى في Outlook 2003.

٢. قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الخاص بك.

٣. في صفحة "Certificate Installed" ("تم تثبيت الشهادة")، انقر فوق **Next (التالي)**.

٤. في صفحة "Certificate Backup" ("النسخ الاحتياطي للشهادة")، قم بإدخال مكان ملف النسخ الاحتياطي واسمه، أو انقر فوق **Browse (استعراض)** لتحديد مكان.

△ **تنبيه:** تأكد من أنك قد قمت بحفظ الملف في مكان آخر بالإضافة إلى القرص الصلب ثم ضعه في مكان آمن. يجب أن يكون هذا الملف مخصص للاستخدام فقط حيث أنه يُطلب إذا كنت في حاجة إلى استعادة Privacy Manager Certificate (شهادة إدارة الخصوصية) الخاصة بك والمفاتيح المقترنة بها.

٥. أدخل كلمة مرور وقم بتأكيدها، ثم انقر فوق **Next (التالي)**.

٦. قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الخاص بك.

٧. إذا اخترت أن تبدأ العملية الخاصة بإرسال دعوة إلى جهات اتصال موثوق بها، فاتبع الإرشادات التي تظهر على الشاشة بادئًا بالخطوة الثانية من الموضوع إضافة جهات اتصال موثوق بها باستخدام جهات الاتصال الموجودة في Microsoft Outlook في صفحة ٤٧.

– أو –

إذا قمت بالنقر فوق **Cancel (إلغاء)**، فارجع إلى إضافة جهة اتصال موثوق بها في صفحة ٤٦ المزيد من المعلومات حول إضافة جهة اتصال موثوق بها فيما بعد.

عرض تفاصيل Privacy Manager Certificate (شهادة إدارة الخصوصية)

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Certificates (الشهادات)**.

٢. انقر فوق Privacy Manager Certificate (شهادة إدارة الخصوصية).

٣. انقر فوق **Certificate details (تفاصيل الشهادة)**.

٤. فور الانتهاء من عرض التفاصيل، انقر فوق **OK (موافق)**.

تجديد Privacy Manager Certificate (شهادة إدارة الخصوصية)

عندما توشك صلاحية Privacy Manager Certificate (شهادة إدارة الخصوصية) الخاصة بك على الانتهاء، سيتم إعلامك بالحاجة إلى تجديدها:

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Certificates (الشهادات)**.

٢. انقر فوق **Renew certificate (تجديد الشهادة)**.

٣. اتبع الإرشادات التي تظهر على الشاشة لشراء Privacy Manager Certificate (شهادة إدارة الخصوصية) جديدة.

ملاحظة: لا تقوم عملية تجديد Privacy Manager Certificate (شهادة إدارة الخصوصية) باستبدال Privacy Manager Certificate (شهادة إدارة الخصوصية) القديمة. ستحتاج إلى شراء Privacy Manager Certificate (شهادة إدارة الخصوصية) جديدة وتثبيتها متبعًا نفس الإجراءات المستخدمة في طلب Privacy Manager Certificate (شهادة إدارة الخصوصية) وتثبيتها في صفحة ٤٢.

تعيين Privacy Manager Certificate (شهادة إدارة الخصوصية) افتراضية

تعد Privacy Manager Certificates (شهادات إدارة الخصوصية) الشهادات الوحيدة المرئية من داخل Privacy Manager (إدارة الخصوصية) حتى في حالة وجود شهادات إضافية خاصة بسلطات الشهادات مثبتة على جهاز الكمبيوتر الخاص بك.

إذا كان يوجد لديك أكثر من Privacy Manager Certificate (شهادة إدارة الخصوصية) مثبتة من داخل Privacy Manager (إدارة الخصوصية)، فيمكنك تحديد إحداها على أن تكون الشهادة الافتراضية:

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Certificates (الشهادات)**.

٢. انقر فوق Privacy Manager Certificate (شهادة إدارة الخصوصية) التي ترغب في أن تكون الشهادة الافتراضية المستخدمة، ثم انقر فوق **Set default (التعيين افتراضيًا)**.

٣. انقر فوق **OK (موافق)**.

ملاحظة: ليس مطلوبًا منك استخدام Privacy Manager Certificate (شهادة إدارة الخصوصية) الخاصة بك. من داخل وظائف Privacy Manager (إدارة الخصوصية) المتعددة، يمكنك تحديد إحدى Privacy Manager Certificates (شهادات إدارة الخصوصية) الخاصة بك لاستخدامها.

حذف Privacy Manager Certificate (شهادة إدارة الخصوصية)

إذا قمت بحذف إحدى Privacy Manager Certificate (شهادة إدارة الخصوصية)، فإنك لن تتمكن من فتح أي ملفات أو عرض أي بيانات قمت بتشفيرها في هذه الشهادة. إذا قمت بحذف إحدى Privacy Manager Certificate (شهادة إدارة الخصوصية) بطريق الخطأ، فيمكنك استعادتها مستخدمًا ملف النسخ الاحتياطي الذي قمت بإنشاءه عند قيامك بتثبيت الشهادة. راجع استعادة Privacy Manager Certificate (شهادة إدارة الخصوصية) في صفحة ٤٥ للمزيد من المعلومات.

لحذف Privacy Manager Certificate (شهادة إدارة الخصوصية):

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Certificates (الشهادات)**.

٢. انقر فوق Privacy Manager Certificate (شهادة إدارة الخصوصية) التي ترغب في حذفها، ثم انقر فوق **Advanced (متقدم)**.

٣. انقر فوق **Delete (حذف)**.

٤. عند ظهور مربع حوار التأكيد، انقر فوق **Yes** (نعم).

٥. انقر فوق **Close** (إغلاق)، ثم فوق **Apply** (تطبيق).

استعادة Privacy Manager Certificate (شهادة إدارة الخصوصية)

أثناء تثبيت Privacy Manager Certificate (شهادة إدارة الخصوصية) الخاصة بك، سيطلب منك إنشاء نسخة احتياطية من الشهادة. يمكنك أيضًا إنشاء نسخة احتياطية من خلال صفحة Migration (الترحيل) يمكنك استخدام هذه النسخة الاحتياطية عند الانتقال إلى جهاز كمبيوتر آخر أو لاستعادة إحدى الشهادات على نفس الكمبيوتر.

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Migration (ترحيل)**.

٢. انقر فوق **Restore (استعادة)**.

٣. في صفحة "Migration File" ("ملف الترحيل")، انقر فوق **Browse (استعراض)** للبحث عن ملف .dppsm الذي قمت بإنشاءه أثناء عملية النسخ الاحتياطي، ثم انقر فوق **Next (التالي)**.

٤. أدخل كلمة المرور التي استخدمتها عند قيامك بإنشاء النسخ الاحتياطي، ثم انقر فوق **Next (التالي)**.

٥. انقر فوق **Finish (إنهاء)**.

٦. انقر فوق **OK (موافق)**.

راجع تثبيت Privacy Manager Certificate (شهادة إدارة الخصوصية) في صفحة ٤٣ أو عمل نسخ احتياطي لـPrivacy Manager Certificates (شهادات إدارة الخصوصية) و Trusted Contacts (جهات الاتصال الموثوق بها) في صفحة ٥٩ للمزيد من المعلومات.

إلغاء Privacy Manager Certificate (شهادة إدارة الخصوصية)

إذا شعرت بأن الأمن الخاص بـPrivacy Manager Certificate (شهادة إدارة الخصوصية) الخاصة بك عرضة للخطر، فيمكنك إلغاء الشهادة الخاصة بك:

ملاحظة: لا يتم حذف Privacy Manager Certificate (شهادة إدارة الخصوصية) التي تم إلغاءها. حيث يمكن استخدام الشهادة لعرض الملفات المشفرة.

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Certificates (الشهادات)**.

٢. انقر فوق **Advanced** (متقدم).

٣. انقر فوق Privacy Manager Certificate (شهادة إدارة الخصوصية) التي ترغب في إلغاءها، ثم انقر فوق **Revoke (إلغاء)**.

٤. عند ظهور مربع حوار التأكيد، انقر فوق **Yes** (نعم).

٥. قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الخاص بك.

٦. اتبع الإرشادات التي تظهر على الشاشة.

إدارة جهات الاتصال الموثوق بها

جهات الاتصال الموثوق بها هم المستخدمين الذين قمت بتبادل Privacy Manager Certificates (شهادات إدارة الخصوصية) معهم والذين يقومون بتمكينك من الاتصال بأمان مع بعضكم البعض.

تسمح لك Trusted Contacts Manager (إدارة جهات الاتصال الموثوق بها) من إجراء المهام التالية:

- عرض تفاصيل جهات الاتصال الموثوق بها
- حذف جهات اتصال موثوق بها
- التحقق من حالة إلغاء جهات اتصال موثوق بها (متقدم)

إضافة جهات اتصال موثوق بها

تتألف عملية إضافة جهات اتصال موثوق بها من 3 خطوات:

١. أن ترسل دعوة عبر البريد الإلكتروني إلى مستلم جهة اتصال موثوق بها.

٢. أن يرد مستلم جهة الاتصال الموثوق بها على البريد الإلكتروني.

٣. أن تستلم رد مستلم جهة الاتصال الموثوق بها على البريد الإلكتروني، ثم تقوم بالنقر فوق **Accept (قبول)**.

يمكنك إرسال دعوات عبر البريد الإلكتروني إلى مستلمين فرديين من جهات الاتصال الموثوق بها أو يمكنك إرسال الدعوة إلى كافة الجهات الموجودة في دفتر العناوين بـMicrosoft Outlook.

راجع الأقسام التالية لإضافة جهات اتصال موثوق بها.

ملاحظة: لكي يتمكن مستلم جهة اتصال موثوق بها من الرد على الدعوة المرسلة إليه بشأن أن يصبح جهة اتصال موثوق بها، يجب أن توجد لديه Privacy Manager (إدارة الخصوصية) مثبتة على الكمبيوتر الخاص به أو يكون لديه عميل بديل مثبت. للمزيد من المعلومات حول تثبيت العميل البديل، قم بزيارة DigitalPersona على موقع الويب على http://DigitalPersona.com/PrivacyManager.

إضافة جهة اتصال موثوق بها

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Trusted Contacts Manager (إدارة جهات الاتصال الموثوق بها)**، ثم انقر فوق **Invite Contacts (إرسال دعوة إلى جهات الاتصال)**.

– أو –

في Microsoft Outlook، انقر فوق السهم إلى الأسفل الموجود بجوار **Send Securely (الإرسال الآمن)** في شريط المهام، ثم انقر فوق **Invite Contacts (إرسال دعوة إلى جهات الاتصال)**.

٢. إذا تم ظهور مربع الحوار Select Certificate (تحديد الشهادة)، فانقر فوق Privacy Manager Certificate (شهادة إدارة الخصوصية) التي ترغب في استخدامها ثم انقر فوق **OK (موافق)**.

٣. عندما يتم ظهور مربع الحوار Trusted Contact Invitation (إرسال دعوة إلى جهات اتصال موثوق بها)، قم بقراءة النص، ثم انقر فوق **OK (موافق)**.

سيتم إنشاء بريد إلكتروني تلقائيًا.

٤. أدخل عنوان بريد إلكتروني أو أكثر للمستلمين الذين تريد إضافتهم كجهات اتصال موثوق بها.

٥. قم بتحرير النص والتوقيع باسمك (اختياري).

٦. انقر فوق **Send** (إرسال).

ملاحظة: إذا لم تكن قد حصلت على Privacy Manager Certificate (شهادة إدارة الخصوصية)، فستظهر رسالة لتخبرك بضرورة وجود Privacy Manager Certificate (شهادة إدارة الخصوصية) لديك كي تتمكن من إرسال طلب جهة اتصال. انقر فوق **OK (موافق)** لإطلاق Certificate Request Wizard (معالج طلب الشهادة). راجع طلب Privacy Manager Certificate (شهادة إدارة الخصوصية) وتثبيتها في صفحة ٤٢ للمزيد من المعلومات.

٧. قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الخاص بك.

ملاحظة: عند استلام جهة الاتصال الموثوق بها للرسالة الإلكترونية، يجب على المستلم أن يقوم بفتح الرسالة الإلكترونية وينقر فوق **Accept (قبول)** في الزاوية السفلى اليمنى من الرسالة الإلكترونية، ثم ينقر فوق **OK (موافق)** عندما يتم ظهور مربع حوار التأكيد.

٨. عند استلامك رد المستلم عبر البريد الإلكتروني بقبول دعوة أن يصبح جهة اتصال موثوق بها، انقر فوق **Accept** (قبول) في الزاوية السفلى اليمنى من البريد الإلكتروني.

يتم ظهور مربع حوار لتأكيد إضافة المستلم بنجاح إلى قائمة جهات الاتصال الموثوق بها.

٩. انقر فوق **OK (موافق)**.

إضافة جهات اتصال موثوق بها باستخدام جهات الاتصال الموجودة في Microsoft Outlook

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Trusted Contacts Manager (إدارة جهات الاتصال الموثوق بها)**، ثم انقر فوق **Invite Contacts (إرسال دعوة إلى جهات الاتصال)**.

– أو –

في Microsoft Outlook، انقر فوق السهم إلى الأسفل الموجود بجوار **Send Securely (الإرسال الآمن)** في شريط المهام، ثم انقر فوق **All My Outlook Contacts (كافة جهات الاتصال الخاصة بي الموجودة في Outlook)**.

٢. عندما يتم فتح صفحة "Trusted Contact Invitation" ("إرسال دعوة إلى جهات اتصال موثوق بها")، قم بتحديد عناوين البريد الإلكتروني الخاصة بالمستلمين الذين ترغب في إضافتهم كجهات اتصال موثوق بها ثم انقر فوق **Next (التالي)**.

٣. في صفحة "Sending Invitation" ("إرسال الدعوة")، انقر فوق **Finish (إنهاء)**.

سيتم تلقائيًا إنشاء بريد إلكتروني مسرود به عناوين البريد الإلكتروني المحددة والموجودة في Microsoft Outlook.

٤. قم بتحرير النص والتوقيع باسمك (اختياري).

٥. انقر فوق **Send** (إرسال).

ملاحظة: إذا لم تكن قد حصلت على Privacy Manager Certificate (شهادة إدارة الخصوصية)، فستظهر رسالة لتخبرك بضرورة وجود Privacy Manager Certificate (شهادة إدارة الخصوصية) لديك كي تتمكن من إرسال طلب جهة اتصال. انقر فوق **OK (موافق)** لإطلاق Certificate Request Wizard (معالج طلب الشهادة). راجع طلب Privacy Manager Certificate (شهادة إدارة الخصوصية) وتثبيتها في صفحة ٤٢ للمزيد من المعلومات.

٦. قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الخاص بك.

ملاحظة: عند استلام جهة الاتصال الموثوق بها للرسالة الإلكترونية، يجب على المستلم أن يقوم بفتح الرسالة الإلكترونية وينقر فوق **Accept (قبول)** في الزاوية السفلى اليمنى من الرسالة الإلكترونية، ثم ينقر فوق **OK (موافق)** عندما يتم ظهور مربع حوار التأكيد.

٧. عند استلامك رد المستلم عبر البريد الإلكتروني بقبول دعوة أن يصبح جهة اتصال موثوق بها، انقر فوق **Accept** (قبول) في الزاوية السفلى اليمنى من البريد الإلكتروني.

يتم ظهور مربع حوار لتأكيد إضافة المستلم بنجاح إلى قائمة جهات الاتصال الموثوق بها.

٨. انقر فوق **OK (موافق)**.

عرض تفاصيل جهات الاتصال الموثوق بها

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Trusted Contacts (جهات الاتصال الموثوق بها)**.

٢. انقر فوق إحدى جهات الاتصال الموثوق بها.

٣. انقر فوق **Contact details (تفاصيل جهة الاتصال)**.

٤. فور الانتهاء من عرض التفاصيل، انقر فوق **OK (موافق)**.

حذف جهة اتصال موثوق بها

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Trusted Contacts (جهات الاتصال الموثوق بها)**.

٢. انقر فوق جهة الاتصال التي تريد حذفها.

٣. انقر فوق **Delete contact (حذف جهة الاتصال)**.

٤. عند ظهور مربع حوار التأكيد، انقر فوق **Yes** (نعم).

التحقق من حالة إلغاء جهة اتصال موثوق بها

لمعرفة ما إذا قد قامت إحدى جهات الاتصال الموثوق بها بإلغاء Privacy Manager Certificate (شهادة إدارة الخصوصية) الخاصة بها:

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Trusted Contacts (جهات الاتصال الموثوق بها)**.

٢. انقر فوق إحدى جهات الاتصال الموثوق بها.

٣. انقر فوق زر **Advanced (متقدم)**.

يتم ظهور مربع الحوار Advanced Trusted Contact Management (إدارة جهات الاتصال الموثوق بها المتقدمة).

٤. انقر فوق **Check Revocation** (التحقق من الإلغاء).

٥. انقر فوق **Close** (إغلاق).

مهام عامة

يمكنك استخدام Privacy Manager (إدارة الخصوصية) مع منتجات Microsoft التالية:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

استخدام Privacy Manager (إدارة الخصوصية) في Microsoft Outlook

عندما يتم تثبيت Privacy Manager (إدارة الخصوصية)، سيتم عرض زر Privacy (الخصوصية) في شريط المهام الموجود في Microsoft Outlook، كما سيتم عرض زر Send Securely (الإرسال الآمن) في شريط المهام الموجود في كل رسالة بريد إلكتروني خاصة بـMicrosoft Outlook. عندما تقوم بالنقر فوق السهم إلى الأسفل الموجود بجوار **Privacy (الخصوصية)** أو **Send Securely (الإرسال الآمن)**، سيمكنك الاختيار من الخيارات التالية:

- Sign and Send (التوقيع والإرسال (زر Send Securely (الإرسال الآمن) فقط))—يضيف هذا الخيار توقيع رقمي إلى البريد الإلكتروني ويقوم بإرساله بعد قيامك بالمصادقة على استخدام أسلوب تسجيل الدخول الآمن الخاص بك.
- Seal for Trusted Contacts and Send (الختم لجهات الاتصال الموثوق بها والإرسال (زر Send Securely (الإرسال الآمن) فقط))—يضيف هذا الخيار توقيع رقمي إلى البريد الإلكتروني ويقوم بتشفيره وإرساله بعد قيامك بالمصادقة على استخدام أسلوب تسجيل الدخول الآمن الخاص بك.
- Invite Contacts (إرسال دعوة إلى جهات الاتصال)—يتيح لك هذا الخيار إرسال دعوة إلى جهة اتصال موثوق بها. راجع إضافة جهة اتصال موثوق بها في صفحة ٤٦ للمزيد من المعلومات.
- Invite Outlook Contacts (إرسال دعوة إلى جهات الاتصال الموجودة في Outlook)—يتيح لك هذا الخيار إرسال دعوة إلى جهة اتصال موثوق بها تشمل كافة جهات الاتصال الموجودة في دفتر عناوين Microsoft Outlook الخاص بك. راجع إضافة جهات اتصال موثوق بها باستخدام جهات الاتصال الموجودة في Microsoft Outlook في صفحة ٤٧ للمزيد من المعلومات.
- قم بفتح برنامج Privacy Manager (إدارة الخصوصية)—تتيح لك خيارات Certificates (الشهادات)، و Trusted Contacts (جهات الاتصال الموثوق بها)، و Settings (الإعدادات) فتح برنامج Privacy Manager (إدارة الخصوصية) لإضافة الإعدادات الحالية أو عرضها أو تغييرها. راجع تكوين Privacy Manager (إدارة الخصوصية) في Microsoft Outlook في صفحة ٤٩ للمزيد من المعلومات.

تكوين Privacy Manager (إدارة الخصوصية) في Microsoft Outlook

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Settings (إعدادات)**، ثم انقر فوق علامة التبويب **E-mail (البريد الإلكتروني)**.

– أو –

في شريط المهام الرئيسي الموجود في Microsoft Outlook، انقر فوق السهم إلى الأسفل الموجود بجوار **Send Securely (الإرسال الآمن)** (**Privacy (الخصوصية)** في Outlook 2003)، ثم انقر فوق **Settings (إعدادات)**.

– أو –

في شريط المهام الموجود بأي من رسائل البريد الإلكتروني في Microsoft Outlook، انقر فوق السهم إلى الأسفل الموجود بجوار **Send Securely (الإرسال الآمن)**، ثم انقر فوق **Settings (إعدادات)**.

٢. حدد الإجراءات التي ترغب في تنفيذها عندما تقوم بإرسال بريد إلكتروني آمن، ثم انقر فوق **OK (موافق)**.

توقيع وإرسال رسالة بريد إلكتروني

١. في Microsoft Outlook، انقر فوق **New (رسالة جديدة)** أو **Reply (الرد على الرسالة)**.

٢. قم بكتابة رسالة البريد الإلكتروني.

٣. انقر فوق السهم إلى الأسفل الموجود بجوار **Send Securely (الإرسال الآمن)** (**Privacy (الخصوصية)** في Outlook 2003)، ثم انقر فوق **Sign and Send (التوقيع والإرسال)**.

٤. قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الخاص بك.

ختم وإرسال رسالة بريد إلكتروني

يمكن فقط للأشخاص الذين تختارهم من قائمة جهات الاتصال الموثوق بها الخاصة بك عرض رسائل البريد الإلكتروني المختومة التي تم توقيعها وختمها (تشفيرها) رقميًا.

لختم رسالة بريد إلكتروني وإرسالها إلى جهة اتصال موثوق بها:

١. في Microsoft Outlook، انقر فوق **New (رسالة جديدة)** أو **Reply (الرد على الرسالة)**.

٢. قم بكتابة رسالة البريد الإلكتروني.

٣. انقر فوق السهم إلى الأسفل الموجود بجوار **Send Securely (الإرسال الآمن)** (**Privacy (الخصوصية)** في Outlook 2003)، ثم انقر فوق **Seal for Trusted Contacts and Send (التوقيع لجهات الاتصال الموثوق بها والإرسال)**.

٤. قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الخاص بك.

عرض رسالة بريد إلكتروني مختومة

عندما تقوم بفتح رسالة بريد إلكتروني مختومة، يتم عرض ملصق الأمن في عنوان البريد الإلكتروني. يقوم ملصق الأمن بتوفير المعلومات التالية:

- بيانات الاعتماد التي تم استخدامها للتحقق من هوية الشخص الذي قام بالتوقيع على البريد الإلكتروني
- المنتج الذي تم استخدامه للتحقق من بيانات الاعتماد الخاصة بالشخص الذي قام بالتوقيع على البريد الإلكتروني

استخدام Privacy Manager (إدارة الخصوصية) في مستند Microsoft Office 2007

ملاحظة: يمكن استخدام Privacy Manager (إدارة الخصوصية) فقط مع مستندات Microsoft Office 2007.

بعد أن تقوم بتثبيت Privacy Manager Certificate (شهادة إدارة الخصوصية) الخاصة بك، سيتم عرض زر Sign and Encrypt (التوقيع والتشفير) في الجانب الأيمن من شريط المهام الموجود في كافة مستندات Microsoft Word، و Microsoft Excel، و Microsoft PowerPoint. عندما تقوم بالنقر فوق السهم إلى الأسفل الموجود بجوار **Sign and Encrypt (التوقيع والتشفير)**، سيمكنك الاختيار من الاختيارات التالية:

- Sign Document (توقيع المستند)—يقوم هذا الخيار بإضافة التوقيع الرقمي الخاص بك إلى المستند.
- Add Signature Line Before Signing (إضافة سطر للتوقيع قبل التوقيع) (Microsoft Word only) و Microsoft Excel فقط)—حسب الإعدادات الافتراضية، فإنه تتم إضافة سطر للتوقيع عند توقيع أو تشفير مستند Microsoft Word أو Microsoft Excel. لإيقاف تشغيل هذا الخيار، انقر فوق **Add Signature Line (إضافة سطر للتوقيع)** لإزالة علامة الاختيار.
- Encrypt Document (تشفير المستند)—يقوم هذا الخيار بإضافة التوقيع الرقمي الخاص بك إلى المستند وتشفيره.
- Remove Encryption (إزالة التشفير)—يقوم هذا الخيار بحذف التشفير من المستند.
- قم بفتح برنامج Privacy Manager (إدارة الخصوصية)—تتيح لك خيارات Certificates (الشهادات)، و Trusted Contacts (جهات الاتصال الموثوق بها)، و Settings (الإعدادات) فتح برنامج Privacy Manager (إدارة الخصوصية) لإضافة الإعدادات الحالية أو عرضها أو تغييرها. راجع إدارة Privacy Manager Certificates (شهادات إدارة الخصوصية) في صفحة ٤٢، إدارة جهات الاتصال الموثوق بها في صفحة ٤٥، أو تكوين Privacy Manager (إدارة الخصوصية) لـMicrosoft Office في صفحة ٥١ للمزيد من المعلومات.

تكوين Privacy Manager (إدارة الخصوصية) لـMicrosoft Office

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Settings (إعدادات)**، ثم انقر فوق علامة التبويب **Documents (المستندات)**.

– أو –

في شريط المهام الموجود بأي من مستندات Microsoft Office، انقر فوق السهم إلى الأسفل الموجود بجوار **Sign and Encrypt (التوقيع والتشفير)**، ثم انقر فوق **Settings (إعدادات)**.

٢. حدد الإجراءات التي تريد تكوينها، ثم انقر فوق **OK (موافق)**.

توقيع مستند Microsoft Office

١. في Microsoft Word أو Microsoft Excel أو Microsoft PowerPoint قم بإنشاء مستند وحفظه.

٢. انقر فوق السهم إلى الأسفل الموجود بجوار **Sign and Encrypt (التوقيع والتشفير)**، ثم انقر فوق **Sign Document (توقيع المستند)**.

٣. قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الخاص بك.

٤. عندما يتم ظهور مربع حوار التأكيد، قم بقراءة النص، ثم انقر فوق **OK (موافق)**.

إذا قررت فيما بعد تحرير المستند، فقم باتباع الخطوات التالية:

١. انقر فوق زر **Office (المستند)** الموجود في الزاوية العليا اليسرى من الشاشة.

٢. انقر فوق **Prepare (تحضير)**، ثم فوق **Mark as Final (التمييز كوضع نهائي)**.

٣. عند ظهور مربع حوار التأكيد، انقر فوق **Yes (نعم)**، وقم بمواصلة الإجراءات.

٤. عندما تنتهي من عملية التحرير، قم بالتوقيع على المستند مرة أخرى.

إضافة سطر للتوقيع عند توقيع مستند Microsoft Word أو Microsoft Excel

تتيح لك Privacy Manager (إدارة الخصوصية) إضافة سطر للتوقيع عند توقيع مستند Microsoft Word أو Microsoft Excel:

١. في Microsoft Word أو Microsoft Excel قم بإنشاء مستند وحفظه.

٢. انقر فوق قائمة **Home** (الصفحة الرئيسية).

٣. انقر فوق السهم إلى الأسفل الموجود بجوار **Sign and Encrypt (التوقيع والتشفير)**، ثم انقر فوق **Add Signature Line Before Signing (إضافة سطر للتوقيع قبل التوقيع)**.

ملاحظة: يتم عرض علامة اختيار بجوار Add Signature Line Before Signing (إضافة سطر للتوقيع قبل التوقيع) عند تحديد هذا الخيار. هذا الخيار في حالة تمكين طبقًا للإعدادات الافتراضية.

٤. انقر فوق السهم إلى الأسفل الموجود بجوار **Sign and Encrypt (التوقيع والتشفير)**، ثم انقر فوق **Sign Document (توقيع المستند)**.

٥. قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الخاص بك.

إضافة موقعين مقترحين عند توقيع مستند Microsoft Word أو Microsoft Excel

يمكنك إضافة أكثر من سطر للتوقيع إلى المستند الخاص بك من خلال تعيين موقعين مقترحين. الموقع المقترح هو مستخدم يقوم بتعيينه مالك مستند Microsoft Word أو Microsoft Excel لإضافة سطر للتوقيع إلى المستند. يمكنك أن تكون الموقع المقترح أو أن يكون الموقع أي شخص آخر تريد منه القيام بتوقيع المستند الخاص بك. على سبيل المثال، إذا قمت بتحضير إحدى المستندات المطلوب قيام كافة أعضاء القسم لديك بتوقيعها، فيمكنك تضمين سطور للتوقيع لهؤلاء المستخدمين في أسفل الصفحة الأخيرة من المستند مع الإرشادات الخاصة بالتوقيع بتاريخ محدد.

لإضافة موقع مقترح إلى مستند Microsoft Word أو Microsoft Excel:

١. في Microsoft Word أو Microsoft Excel قم بإنشاء مستند وحفظه.

٢. انقر فوق قائمة **Insert** (إدراج).

٣. في مجموعة **Text (النص)** الموجودة في شريط المهام، انقر فوق السهم الموجود بجوار **Signature Line (سطر للتوقيع)**، ثم انقر فوق **Privacy Manager Signature Provider (مزود التوقيع الخاص بإدارة الشهادة)**.

يتم فتح مربع الحوار Signature Setup (إعداد التوقيع).

٤. في المربع الموجود تحت **Suggested signer (الموقع المقترح)**، أدخل اسم الموقع المقترح.

٥. في المربع الموجود تحت **Instructions to the signer (إرشادات إلى الموقع)**، أدخل رسالة لهذا الموقع المقترح.

ملاحظة: ستظهر هذه الرسالة في مكان إحدى العناوين وسيتم إما حذفها أو استبدالها بواسطة'عنوان المستخدم عند توقيع المستند.

٦. حدد **Show sign date (عرض تاريخ التوقيع)** في مربع اختيار سطر التوقيع لعرض التاريخ.

٧. حدد **Show signer's title (عرض عنوان الموقع)** في مربع اختيار سطر التوقيع لعرض العنوان.

ملاحظة: نظرًا لقيام مالك المستند بتعيين موقعين مقترحين إلى المستند الخاص به، فإذا لم يتم تحديد مربعات اختيار **Show sign date (عرض تاريخ التوقيع) في سطر التوقيع** و/أو **Show signer's title (عرض عنوان الموقع) في سطر التوقيع** فلن يتمكن الموقع المقترح من عرض التاريخ و/أو العنوان في سطر التوقيع حتى في حالة تكوين إعدادات المستند الخاص بالموقع المقترح بالقيام بذلك.

٨. انقر فوق **OK (موافق)**.

إضافة سطر للتوقيع للموقعين المقترحين

عند قيام الموقعين المقترحين بفتح المستند، فإنهم سيقومون برؤية أسماءهم في الأقواس، مما يشير إلى ضرورة قيامهم بالتوقيع.

لتوقيع المستند:

١. انقر نقرًا مزدوجًا فوق سطر التوقيع المناسب.

٢. قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الخاص بك.

سيتم عرض سطر التوقيع طبقًا للإعدادات التي حددها مالك المستند.

تشفير إحدى مستندات Microsoft Office

يمكنك تشفير إحدى مستندات Microsoft Office لك أو لجهات الاتصال الموثوق بها الخاصة بك. عندما تقوم بتشفير إحدى المستندات وغلقه، فسيجب عليك وعلى جهات الاتصال الموثوق بها التي تحددها من القائمة المصادقة قبل فتح هذا المستند.

لتشفير إحدى مستندات Microsoft Office:

١. في Microsoft Word أو Microsoft Excel أو Microsoft PowerPoint قم بإنشاء مستند وحفظه.

٢. انقر فوق قائمة **Home** (الصفحة الرئيسية).

٣. انقر فوق السهم إلى الأسفل الموجود بجوار **Sign and Encrypt (التوقيع والتشفير)**، ثم انقر فوق **Encrypt Document (تشفير المستند)**.

يتم ظهور مربع الحوار Select Trusted Contacts (تحديد جهات الاتصال الموثوق بها).

٤. انقر فوق اسم جهة الاتصال الموثوق بها التي ستتمكن من فتح المستند وعرض محتوياته.

ملاحظة: لتحديد عدة أسماء لجهات اتصال موثوق بها، اضغط باستمرار على مفتاح ctrl وانقر فوق أسماء الأفراد.

٥. انقر فوق **OK (موافق)**.

إذا قررت فيما بعد تحرير المستند، فقم باتباع الخطوات التالية لإزالة تشفير إحدى مستندات Microsoft Office في صفحة ٥٣. عندما يتم إزالة التشفير، يمكنك تحرير المستند. قم باتباع الخطوات الموجودة في هذا القسم لتشفير المستند من جديد.

لإزالة تشفير إحدى مستندات Microsoft Office

عندما تقوم بإزالة التشفير من إحدى مستندات Microsoft Office، لن يتطلب منك أو من جهات الاتصال الموثوق بها الخاصة بك بعد ذلك المصادقة على فتح محتويات المستند وعرضها.

لإزالة تشفير من إحدى مستندات Microsoft Office:

١. قم بفتح مستند Microsoft Word أو Microsoft Excel أو Microsoft PowerPoint مشفر.

٢. قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الخاص بك.

٣. انقر فوق قائمة **Home** (الصفحة الرئيسية).

٤. انقر فوق السهم إلى الأسفل الموجود بجوار **Sign and Encrypt (التوقيع والتشفير)**، ثم انقر فوق **Remove Encryption (إزالة التشفير)**.

إرسال مستند Microsoft Office مشفر

يمكن إرفاق مستند Microsoft Office مشفر برسالة بريد إلكتروني دون التوقيع على البريد الإلكتروني نفسه أو تشفيره. للقيام بذلك، قم بإنشاء بريد إلكتروني وإرساله مع مستند تم التوقيع عليه وتشفيره كأنك تقوم بإرسال بريد إلكتروني تقليدي يوجد به مرفقات.

على الرغم من ذلك، ولتحقيق الأمن الأمثل، يوصى بأن تقوم بتشفير البريد الإلكتروني عند إرفاق مستند Microsoft Office تم التوقيع عليه أو تشفيره.

لإرسال بريد إلكتروني مختوم مع مستند Microsoft Office تم التوقيع عليه و/أو تشفيره، قم باتباع الخطوات التالية:

١. في Microsoft Outlook، انقر فوق **New (رسالة جديدة)** أو **Reply (الرد على الرسالة)**.

٢. قم بكتابة رسالة البريد الإلكتروني.

٣. قم بإرفاق مستند Microsoft Office.

٤. راجع ختم وإرسال رسالة بريد إلكتروني في صفحة ٥٠ للمزيد من الإرشادات.

عرض مستند Microsoft Office تم التوقيع عليه

ملاحظة: لن تحتاج إلى وجود Privacy Manager Certificate (شهادة إدارة الخصوصية) كي تتمكن من عرض مستند Microsoft Office تم التوقيع عليه.

عندما يتم فتح مستند Microsoft Office تم التوقيع عليه، سيتم عرض رمز توقيع رقمي في شريط الحالة الموجود في أسفل إطار المستند.

١. انقر فوق رمز **Digital Signatures (التوقيعات الرقمية)** للتبديل بين عرض مربع حوار Signatures (التوقيعات) الذي يعرض أسماء جميع المستخدمين الذين قاموا بالتوقيع على المستند والتاريخ الذي قام فيه كل مستخدم بالتوقيع عليه.

٢. لعرض تفاصيل إضافية بشأن كل توقيع، انقر بزر الماوس الأيمن فوق أي اسم موجود في مربع حوار Signatures (التوقيعات) ثم حدد Signature Details (تفاصيل التوقيع).

عرض مستند Microsoft Office مشفر

لعرض مستند Microsoft Office مشفر من على جهاز كمبيوتر آخر، يجب تثبيت Privacy Manager (إدارة الخصوصية) على ذلك الكمبيوتر. علاوة على ذلك، يجب أن تقوم باستعادة Privacy Manager Certificate (شهادة إدارة الخصوصية) التي تم استخدامها لتشفير الملف.

كي تتمكن أي جهة اتصال موثوق بها من عرض مستند Microsoft Office مشفر، يجب أن تكون لديها Privacy Manager Certificate (شهادة إدارة الخصوصية) وأن تكون Privacy Manager (إدارة الخصوصية) مثبتة على جهاز الكمبيوتر لديها. علاوة على ذلك، يجب أن يقوم مالك مستند Microsoft Office المشفر بتحديد جهة الاتصال الموثوق بها.

استخدام Privacy Manager (إدارة الخصوصية) في برنامج Windows Live Messenger

تضيف Privacy Manager (إدارة الخصوصية) ميزات الاتصالات الآمنة التالية إلى برنامج Windows Live Messenger:

- **Secure chat (المحادثة الفورية الآمنة)**—يتم نقل الرسائل بواسطة SSL/TLS (Secure Sockets Layer/Transport Layer Security) عبر بروتوكول XML وهي نفس التقنية المستخدمة لضمان أمن صفقات التجارة الإلكترونية.
- **Recipient identification (تعريف المستخدم)**—يمكنك التحقق من وجود جهة الاتصال وهويتها قبل القيام بإرسال أي رسائل.
- **Signed messages (الرسائل الموقعة)**—يمكن التوقيع على الرسائل الخاصة بك إلكترونيًا. ثم، إذا عبث أحدهم في الرسالة أحد، فسيتم تعليمها كغير صالحة عند استقبالها على يدي المستقبل.
- **Hide/show feature ميزة (إخفاء/عرض)**—يمكنك إخفاء أي من الرسائل الموجودة في إطار Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية) أو إخفاءها جميعًا. كما يمكن إرسال رسالة حيث يكون المحتوى مخفيًا. سيطلب منك المصادقة قبل عرض الرسالة.
- **Secure chat history (سجل المحادثات الفورية)**—يتم تشفير سجلات المحادثات الفورية الخاصة بك قبل حفظها وهي تتطلب المصادقة كي يتم عرضها.
- **Automatic locking/unlocking (قفل/إلغاء قفل تلقائي)**—يمكن قفل إطار Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية) وإلغاء قفله أو تعيينه على القفل تلقائيًا بعد مرور فترة معينة من عدم النشاط.

بدء جلسة Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية)

ملاحظة: كي تتمكن من استخدام Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية)، يجب تثبيت Privacy Manager (إدارة الخصوصية) و Privacy Manager Certificate (شهادة إدارة الخصوصية) لدى الطرفين. لمعرفة مزيد من التفاصيل بشأن تثبيت Privacy Manager Certificate (شهادة إدارة الخصوصية)، راجع طلب Privacy Manager Certificate (شهادة إدارة الخصوصية) وتثبيتها في صفحة ٤٢.

١. لبدء Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية) في برنامج Windows Live Messenger، قم بتنفيذ إحدى الإجراءات التالية:

أ. انقر بزر الماوس الأيمن فوق إحدى جهات الاتصال المتصلة، ثم حدد **Start an Activity (بدء الأنشطة)**.

ب. انقر فوق **Start Chat** (بدء المحادثة الفورية).

– أو –

أ. انقر نقرًا مزدوجًا فوق جهة اتصال متصلة في برنامج Live Messenger، ثم حدد القائمة **See a list of activities** (عرض قائمة بالأنشطة).

ب. انقر فوق **Action** (الإجراءات)، ثم انقر فوق **Start Chat** (بدء المحادثة الفورية).

– أو –

أ. انقر بزر الماوس الأيمن فوق رمز ProtectTools الموجود في منطقة الإعلام ثم انقر فوق **Privacy Manager for HP ProtectTools (إدارة الخصوصية لـHP ProtectTools)**، ثم حدد **Start Chat (بدء المحادثة الفورية)**.

ب. في برنامج Live Messenger انقر فوق **Actions (الإجراءات): Start an Activity (بدء الأنشطة)**، ثم حدد **Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية)**.

ملاحظة: يجب أن يكون كل مستخدم متصلاً في برنامج Live Messenger ويجب ظهور كل مستخدم متصلاً لدى المستخدمين الآخرين في إطار المحادثة الفورية في برنامج Live Messenger. انقر لتحديد مستخدم متصل.

تقوم Privacy Manager (إدارة الخصوصية) بإرسال دعوة إلى جهة الاتصال لبدء Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية). عندما تقوم جهة الاتصال بقبول الدعوة، سيتم فتح إطار Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية). إذا لم تكن Privacy Manager (إدارة الخصوصية) موجودة لدى جهة الاتصال التي استلمت الدعوة، فإنه سيتم مطالبتها بتنزيلها.

٢. انقر فوق **Start (البدء)** لبدء محادثة فورية آمنة.

تكوين Privacy Manager (إدارة الخصوصية) لبرنامج Windows Live Messenger

١. في Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية)، انقر فوق زر **Settings** (إعدادات).

– أو –

في Privacy Manager (إدارة الخصوصية)، انقر فوق **Settings (إعدادات)**، ثم انقر فوق علامة التبويب **Chat (المحادثة الفورية)**.

– أو –

في Privacy Manager Live Messenger History Viewer (عارض سجل برنامج Live Messenger الخاص بإدارة الخصوصية)، انقر فوق زر **Settings** (إعدادات).

٢. لتحديد المدة التي يجب أن تنقضي قبل أن تقوم Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية) بقفل جلستك، حدد رقمًا من المربع **Lock session after _ minutes of inactivity** (قفل الجلسة بعد _ دقائق من عدم النشاط).

٣. لتحديد مجلد خاص بسجل جلسات المحادثة الفورية الخاصة بك، انقر فوق **Browse (استعراض)** لتحديد إحدى المجلدات ثم انقر فوق **OK (موافق)**.

٤. لتشفير الجلسات الخاصة بك وحفظها تلقائيًا عندما تقوم بإغلاقها، حدد مربع الاختيار **Automatically save secure chat history (حفظ سجل المحادثة الفورية الآمنة تلقائيًا)**.

٥. انقر فوق **OK (موافق)**.

التحدث الفوري في إطار Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية)

بعد بدء Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية)، سيتم فتح إطار Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية) في برنامج Windows Live Messenger. يعد استخدام Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية) مماثلاً لاستخدام برنامج Windows Live Messenger الأساسي باستثناء توفر الميزات الإضافية التالية في إطار Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية):

- **Save (حفظ)** –انقر فوق هذا الزر لحفظ جلسة المحادثة الفورية في المجلد المحدد في إعدادات التكوين. كما يمكنك تكوين Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية) ليحفظ تلقائيًا كل جلسة قبل قفلها.
- **Hide all (إخفاء الكل)** و**Show all (إظهار الكل)** –انقر فوق الزر المناسب لفتح أو طي الرسائل الظاهرة في الإطار Secure Communications (اتصالات آمنة). كما يمكنك إظهار أو عرض رسائل فردية بالنقر فوق ترويسة الرسالة.
- **Are you there? (هل أنت موجود؟)** –انقر فوق هذا الزر لطلب المصادقة من جهة الاتصال.
- **Lock (قفل)** –انقر فوق هذا الزر لإغلاق إطار Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية) وللرجوع إلى الإطار Chat Entry (الدخول إلى المحادثة). لعرض الإطار Secure Communications (اتصالات آمنة)، انقر فوق **Resume the session (استئناف الجلسة)**، ثم قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الذي اخترته.
- **Send (إرسال)** –انقر فوق هذا الزر لإرسال رسالة مشفرة إلى جهة الاتصال.
- **Send signed (الإرسال مع التوقيع)** –اختر خانة الاختيار هذه للتوقيع على رسائلك وتشفيرها إلكترونيًا. ثم، إذا عبث أحدهم في الرسالة أحد، فسيتم تعليمها كغير صالحة عند استقبالها على يدي المستقبل. يجب المصادقة كل مرة ترسل فيها رسالة موقعة.
- **Send hidden (الإرسال بعد الإخفاء)** –حدد خانة الاختيار هذه لتشفير وإرسال رسالة مظهرًا ترويستها فقط. يجب أن يقوم جهة الاتصال بالمصادقة لقراءة محتويات الرسالة.

عرض سجل المحادثات

Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية): يقوم Live Messenger History Viewer (عارض سجل برنامج Live Messenger) بعرض الملفات المشفرة الخاصة بجلسة Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية). يمكن حفظ الجلسات بالنقر فوق **Save** (حفظ) في الإطار Privacy Manager Chat (المحادثة الفورية الخاصة بإدارة الخصوصية)، أو بتكوين الحفظ التلقائي في علامة التبويب Chat (محادثة فورية) التي في Privacy Manager (إدارة الخصوصية). في العارض, تظهر كل جلسة اسم العرض (المشفر) لجهة الاتصال والموعد والساعة الذين بدأت الجلسة بهما وانتهت. افتراضيًا, تعرض الجلسات بالنسبة إلى كافة حسابات البريد الإلكتروني التي أعددتها. يمكنك استخدام القائمة **Display history for** (عرض السجل الخاص بـ) لتحديد حسابات معينة للعرض.

يتيح لك العارض إجراء المهام التالية:

- كشف كافة الجلسات في صفحة ٥٦
- كشف الجلسات الخاصة بحساب محدد في صفحة ٥٦
- عرض معرف الجلسة في صفحة ٥٧
- عرض الجلسة في صفحة ٥٧
- البحث عن الجلسات التي تحتوي على نص محدد في صفحة ٥٧
- حذف الجلسة في صفحة ٥٧
- إضافة أو إزالة الأعمدة في صفحة ٥٨
- تنقيح الجلسات المعروضة في صفحة ٥٨

لبدء Live Messenger History Viewer (عارض سجل برنامج Live Messenger):

▲ في منطقة الإعلام الموجودة في أقصى يمين شريط المهام، انقر بزر الماوس الأيمن فوق رمز **HP ProtectTools** ثم انقر فوق **Privacy Manager (إدارة الخصوصية)**: لـ**HP ProtectTools** ثم انقر فوق **Live Messenger History Viewer (عارض سجل برنامج Live Messenger)**.

– أو –

▲ في جلسة Chat (المحادثة الفورية) انقر فوق **History Viewer (عارض السجل)** أو **History (السجل)**.

كشف كافة الجلسات

يؤدي كشف كافة الجلسات إلى عرض اسم العرض الخاص بجهة الاتصال التي تم فك التشفير الخاص بها للجلسات المحددة حاليًا ولكافة الجلسات الموجودة في نفس الحساب.

لكشف كافة جلسات سجل المحادثة الفورية الخاصة بك والتي تم حفظها:

١. في Live Messenger History Viewer (عارض سجل برنامج Live Messenger) انقر بزر الماوس الأيمن فوق أي جلسة ثم حدد **Reveal All Sessions (كشف كافة الجلسات)**.

٢. قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الخاص بك.

سيتم فك تشفير أسماء عرض جهة الاتصال.

٣. انقر نقرًا مزدوجًا فوق أي جلسة لعرض محتوياتها.

كشف الجلسات الخاصة بحساب محدد

يؤدي كشف الجلسة إلى عرض اسم العرض الخاص بجهة الاتصال التي تم فك التشفير الخاص بها للجلسات المحددة حاليًا.

لكشف جلسة سجل محادثة فورية محددة:

١. في Live Messenger History Viewer (عارض سجل برنامج Live Messenger) انقر بزر الماوس الأيمن فوق أي جلسة ثم حدد **Reveal Session (كشف الجلسة)**.

٢. قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الخاص بك.

سيتم فك تشفير اسم عرض جهة الاتصال

٣. انقر نقرًا مزدوجًا الجلسة الي تم كشفها لعرض محتوياتها.

ملاحظة: ستقوم الجلسات الإضافية المشفرة التي تحتوي على نفس الشهادة بعرض رمز غير مقفل، لتوضيح إمكانية رؤيتها من خلال النقر نقرًا مزدوجًا فوق أي من تلك الجلسات دون الحاجة إلى مصادقة إضافية. ستقوم الجلسات المشفرة التي تحتوي على شهادة مختلفة بعرض رمز مقفل لتوضيح أن هناك مصادقة إضافية مطلوبة لتلك الجلسات قبل عرض أسماء العرض لجهات الاتصال أو محتوياتها.

عرض معرف الجلسة

لعرض معرف الجلسة:

▲ في Live Messenger History Viewer (عارض سجل برنامج Live Messenger) انقر بزر الماوس الأيمن فوق أي جلسة تم كشفها ثم حدد **View session ID (عرض معرف الجلسة)**.

عرض الجلسة

يؤدي عرض الجلسة إلى فتح الملف المطلوب عرضه. إذا لم يكن قد تم كشف الجلسة (مع عرض اسم عرض جهة الاتصال التي تم فك التشفير الخاص بها) سابقًا، فسيتم كشفها في نفس الوقت.

لعرض جلسة سجل خاصة ببرنامج Live Messenger:

١. في Live Messenger History Viewer (عارض سجل برنامج Live Messenger) انقر بزر الماوس الأيمن فوق أي جلسة ثم حدد **View (عرض)**.

٢. عند المطالبة، قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الخاص بك.

لقد تم فك تشفير المحتوى الخاص بالجلسة.

البحث عن الجلسات التي تحتوي على نص محدد

يمكنك البحث عن نصوص في الجلسات التي تم كشفها (تشفيرها) والمعروضة في إطار العارض فقط. تعد هذه هي الجلسات التي يتم فيها عرض اسم عرض جهة الاتصال في نص عادي.

للبحث عن النصوص في جلسات سجل المحادثات الفورية:

١. في Live Messenger History Viewer (عارض السجل الخاص ببرنامج Live Messenger)، انقر فوق زر **Search** (بحث).

٢. أدخل نص البحث وقم بتكوين أي معلمات تريدها خاصة بالبحث ثم انقر فوق **OK (موافق)**.

يتم تمييز الجلسات التي تحتوي على النص في إطار العارض.

حذف الجلسة

١. حدد جلسة سجل محادثة فورية.

٢. انقر فوق **Delete (حذف)**.

إضافة أو إزالة الأعمدة

حسب الإعدادات الافتراضية فإنه يتم عرض الأعمدة الثلاثة الأكثر استخدامًا في Live Messenger History Viewer (عارض سجل برنامج Live Messenger). يمكنك إضافة أعمدة إضافية إلى العرض أو إزالة أعمدة من العرض.

لإضافة أعمدة إلى العرض:

١. انقر بزر الماوس الأيمن فوق عنوان أي عمود ثم حدد **Add/Remove Columns (إضافة/إزالة أعمدة)**.

٢. حدد إحدى عناوين الأعمدة الموجودة في اللوحة اليسرى ثم انقر فوق**Add (إضافة)** لنقلها إلى اللوحة اليمنى.

لإزالة أعمدة من العرض:

١. انقر بزر الماوس الأيمن فوق عنوان أي عمود ثم حدد **Add/Remove Columns (إضافة/إزالة أعمدة)**.

٢. حدد إحدى عناوين الأعمدة الموجودة في اللوحة اليمنى ثم انقر فوق **Remove (إزالة)** لنقلها إلى اللوحة اليسرى.

تنقيح الجلسات المعروضة

سيتم عرض قائمة من الجلسات بجميع الحسابات الخاصة بك في Live Messenger History Viewer (عارض سجل برنامج Live Messenger). يمكنك أيضًا تنقيح الجلسات المعروضة لما يلي:

- حسابات معينة. للمزيد من التفاصيل، راجع عرض جلسات لحساب محدد في صفحة ٥٨.
- نطاق التواريخ. للمزيد من التفاصيل، راجع عرض الجلسات لنطاق من التواريخ في صفحة ٥٨.
- مجلدات مختلفة. للمزيد من التفاصيل، راجع عرض الجلسات التي حفظها في مجلد آخر غير المجلد الافتراضي في صفحة ٥٨.

عرض جلسات لحساب محدد

▲ في Live Messenger History Viewer (عارض سجل برنامج Live Messenger)، حدد إحدى الحسابات من القائمة **Display history for (عرض السجل الخاص بـ)**.

عرض الجلسات لنطاق من التواريخ

١. في Live Messenger History Viewer (عارض السجل الخاص ببرنامج Live Messenger)، انقر فوق رمز **Advanced Filter** (تنقيح متقدم).

سيتم فتح مربع الحوار Advanced Filter (تنقيح متقدم).

٢. حدد مربع اختيار **عرض الجلسات الموجودة في نطاق محدد من التواريخ**.

٣. في مربعات **From date (من التاريخ)** و**To date (إلى التاريخ)** أدخل اليوم، والشهر، و/أو السنة أو انقر فوق السهم الموجود بجوار التقويم لتحديد التواريخ.

٤. انقر فوق **OK (موافق)**.

عرض الجلسات التي حفظها في مجلد آخر غير المجلد الافتراضي

١. في Live Messenger History Viewer (عارض السجل الخاص ببرنامج Live Messenger)، انقر فوق رمز **Advanced Filter** (تنقيح متقدم).

٢. حدد مربع اختيار **استخدام مجلد خاص بملفات سجل بديل**.

٣. أدخل مكان المجلد أو انقر فوق **Browse (استعراض)** لتحديد إحدى المجلدات.

٤. انقر فوق **OK (موافق)**.

مهام متقدمة

ترحيل Privacy Manager Certificates (شهادات إدارة الخصوصية) وجهات الاتصال الموثوق بها إلى كمبيوتر آخر

يمكنك ترحيل Privacy Manager Certificates (شهادات إدارة الخصوصية) و Trusted Contacts (جهات الاتصال الموثوق بها) الخاصة بك بأمان إلى جهاز كمبيوتر آخر، أو قم بعمل نسخ احتياطي للبيانات الخاصة بك للحماية. للقيام بذلك، قم بعمل نسخ احتياطي للبيانات في صورة ملف وقم بحمايته بكلمة مرور ثم ضعه في مكان بالشبكة أو في أي جهاز تخزين قابل للنقل ثم قم باستعادة الملف إلى جهاز الكمبيوتر الجديد.

عمل نسخ احتياطي لـPrivacy Manager Certificates (شهادات إدارة الخصوصية) و Trusted Contacts (جهات الاتصال الموثوق بها)

لعمل نسخ احتياطي لـPrivacy Manager Certificates (شهادات إدارة الخصوصية) و Trusted Contacts (جهات الاتصال الموثوق بها) في ملف يتم حمايته بكلمة مرور، قم باتباع الخطوات التالية:

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Migration (ترحيل)**.

٢. انقر فوق **Backup (نسخ احتياطي)**.

٣. في صفحة "Select Data" ("تحديد البيانات")، حدد فئات البيانات التي سيتم تضمينها في ملف الترحيل، ثم انقر فوق **Next (التالي)**.

٤. في صفحة "Migration File" ("ملف الترحيل")، أدخل اسم الملف أو انقر فوق **Browse (استعراض)** لتحديد إحدى الأماكن ثم انقر فوق **Next (التالي)**.

٥. أدخل كلمة مرور وقم بتأكيدها، ثم انقر فوق **Next (التالي)**.

ملاحظة: قم بحفظ كلمة المرور هذه في مكان آمن لأنك ستحتاج إليها عندما تقوم باستعادة ملف الترحيل.

٦. قم بالمصادقة مستخدمًا أسلوب تسجيل الدخول الآمن الخاص بك.

٧. في صفحة "Migration File Saved" ("تم حفظ ملف الترحيل")، انقر فوق **Finish (إنهاء)**.

استعادة Privacy Manager Certificates (شهادات إدارة الخصوصية) و Trusted Contacts (جهات الاتصال الموثوق بها)

لاستعادة Privacy Manager Certificates (شهادات إدارة الخصوصية) و Trusted Contacts (جهات الاتصال الموثوق بها) الخاصة بك على جهاز كمبيوتر مختلف كجزء من عملية الترحيل أو على نفس جهاز الكمبيوتر، قم باتباع هذه الخطوات:

١. قم بفتح Privacy Manager (إدارة الخصوصية)، ثم انقر فوق **Migration (ترحيل)**.

٢. انقر فوق **Restore (استعادة)**.

٣. في صفحة "Migration File" ("ملف الترحيل")، انقر فوق **Browse (استعراض)** لتحديد مكان الملف ثم انقر فوق **Next (التالي)**.

٤. أدخل كلمة المرور التي استخدمتها عند قيامك بإنشاء ملف النسخ الاحتياطي، ثم انقر فوق **Next (التالي)**.

٥. في صفحة "Migration File" ("ملف الترحيل")، انقر فوق **Finish (إنهاء)**.

الإدارة المركزية لـPrivacy Manager (إدارة الخصوصية)

يمكن أن تكون عملية تثبيت Privacy Manager (إدارة الخصوصية) التي أجريتها جزءًا من التثبيت المركزي الذي قام المسؤول لديك بتخصيصه. يمكن أن يكون قد تم تمكين أو تعطيل إحدى هذه الميزات أو العديد منها:

- **Certificate use policy (سياسة استخدام الشهادة)**—يمكن أن يتم تقييد استخدامك لـPrivacy Manager Certificate (شهادة إدارة الخصوصية) التي أصدرها Comodo (كومودو) أو ربما قد يتم السماح لك باستخدام الشهادات الرقمية التي أصدرتها سلطات الشهادات الأخرى.
- **Encryption policy** (سياسة التشفير)—يمكن تمكين وتعطيل كل من قدرات التشفير على حدتها في Microsoft Office أو Outlook وفي Windows Live Messenger.

٩ File Sanitizer (أداة تعقيم الملفات) لـHP ProtectTools

File Sanitizer (أداة تعقيم الملفات) هي أداة تتيح لك تقطيع الأصول بأمان (البيانات أو الملفات الشخصية، بيانات السجل أو تلك المستندة إلى الويب أو عناصر البيانات الأخرى) الموجودة في الكمبيوتر كما تتيح لك تبييض محرك الأقراص الثابت دوريًا.

ملاحظة: يدعم هذا الإصدار من File Sanitizer (أداة تعقيم الملفات) محرك الأقراص الثابتة للنظام فقط.

تقطيع

يختلف Shredding (التقطيع) عن الحذف العادي الموجود في نظام التشغيل Windows® (يعرف أيضًا بالحذف البسيط في File Sanitizer (أداة تعقيم الملفات)) أنه عندما تقوم بتقطيع إحدى الأصول باستخدام File Sanitizer (أداة تعقيم الملفات)، يتم استدعاء إحدى الخوارزميات التي تقوم بحجب البيانات مما يجعل من المستحيل فعليًا استعادة الأصول الثابتة. قد يقوم الحذف العادي الموجود في نظام التشغيل Windows بترك الملف (الأصول) سليمًا على القرص الصلب أو في حالة استخدام بعض الأساليب الشرعية فإنه من الممكن استعادة الملف (الأصول).

عندما تقوم باختيار إحدى ملفات تعريف التقطيع (High Security (أمن عالي)، أو Medium Security (أمن متوسط)، أو Low Security (أمن منخفض))، فإنه يتم تلقائيًا تحديد قائمة من الموجودات المحددة مسبقًا وإحدى وسائل المسح للتقطيع. يمكنك أيضًا تخصيص إحدى ملفات تعريف التقطيع التي تسمح لك بتحديد عدد دورات التقطيع والأصول التي سيتم تضمينها في التقطيع والأصول التي سيتم تأكيدها قبل التقطيع والأصول التي سيتم استبعادها من التقطيع. للحصول على مزيد من المعلومات، راجع تحديد أو إنشاء إحدى ملفات تعريف التقطيع في صفحة ٦٥.

يمكنك إعداد جدول تقطيع تلقائي كما يمكنك أيضًا تقطيع الأصول يدويًا متى تريد. للحصول على مزيد من المعلومات، راجع تعيين جدول للتقطيع في صفحة ٦٤، تقطيع إحدى الأصول يدويًا في صفحة ٦٨، أو تقطيع كافة العناصر المحددة يدويًا في صفحة ٦٨.

ملاحظة: يتم تقطيع ملف .dll وإزالته من النظام فقط إذا تم نقله إلى سلة المحذوفات.

تبييض المساحة الحرة

لا يؤدي حذف إحدى الأصول في نظام تشغيل Windows إلى إزالة محتويات الأصول بشكل تام من القرص الصلب. يقوم نظام تشغيل Windows بحذف مرجع الأصول فقط. تظل محتويات الأصول موجودة على القرص الصلب حتى تقوم أصول أخرى بكتابة معلومات جديدة فوق هذه المنطقة من القرص الصلب.

يتيح لك تبييض المساحة الحرة بكتابة بيانات عشوائية فوق الأصول المحذوفة بأمان، وهو ما يمنع المستخدمين من عرض المحتويات الأصلية للأصول المحذوفة.

ملاحظة: يستخدم تبييض المساحة الحرة للأصول التي تقوم بحذفها من خلال Windows Recycle Bin (سلة المحذوفات الموجودة في نظام تشغيل Windows) أو تلك التي تقوم بحذفها يدويًا. لا يوفر تبييض المساحة الحرة أي أمن إضافي إلى الأصول التي تم تقطيعها.

يمكنك تعيين جدول تلقائي خاص بتبييض المساحة الحرة أو يمكنك تنشيط تبييض المساحة الحرة يدويًا من خلال رمز **HP ProtectTools** الموجود في منطقة الإعلام في أقصى يمين شريط المهام. للحصول على مزيد من المعلومات، راجع تعيين جدول خاص بتبييض المساحة الحرة في صفحة ٦٤ أو تنشيط تبييض المساحة الحرة يدويًا في صفحة ٦٨.

إجراءات الإعداد

فتح File Sanitizer (أداة تعقيم الملفات)

لفتح File Sanitizer (أداة تعقيم الملفات):

١. انقر فوق **Start (ابدأ)**، ثم **All Programs (كافة البرامج)**، ثم **HP**، ثم انقر فوق **HP ProtectTools Security Manager (إدارة الحماية لـHP ProtectTools)**.

٢. انقر فوق **File Sanitizer (أداة تعقيم الملفات)**.

– أو –

▲ انقر نقرًا مزدوجًا فوق رمز **File Sanitizer (أداة تعقيم الملفات)** الموجود على سطح المكتب الخاص بك.

– أو –

▲ انقر بزر الماوس الأيمن فوق رمز **HP ProtectTools** الموجود في منطقة الإعلام ، في أقصى يمين شريط المهام، ثم انقر فوق **File Sanitizer (أداة تعقيم الملفات)**، ثم فوق **Open File Sanitizer (فتح أداة تعقيم الملفات)**.

تعيين جدول للتقطيع

ملاحظة: للمزيد من المعلومات حول تحديد إحدى ملفات تعريف التقطيع المحددة مسبقًا أو إنشاء إحدى ملفات تعريف التقطيع، راجع تحديد أو إنشاء إحدى ملفات تعريف التقطيع في صفحة ٦٥.

ملاحظة: للمزيد من المعلومات حول تقطيع الأصول يدويًا، راجع تقطيع إحدى الأصول يدويًا في صفحة ٦٨.

١. افتح File Sanitizer (أداة تعقيم الملفات), وانقر فوق **Shred** (تقطيع).

٢. تحديد إحدى خيارات التقطيع:

- **Windows shutdown (إيقاف تشغيل نظام تشغيل Windows)**—حدد هذا الخيار لتقطيع كافة الأصول المحددة عند إيقاف تشغيل نظام تشغيل Windows.

ملاحظة: عند تحديد هذا الخيار, يعرض مربع حوار عند إيقاف التشغيل يسألك هل تريد المتابعة في تقطيع الأصول المحددة أو إذا أردت تجنب الإجراء. انقر فوق **Yes (نعم)** لتجنب إجراء التقطيع أو فوق **No (لا)** للمتابعة في التقطيع.

- **Web browser open (فتح مستعرض الويب)**—حدد هذا الخيار لتقطيع كافة الأصول المرتبطة بالويب مثل سجل عنوان URL الخاص بالمستعرض عندما تقوم بفتح إحدى مستعرضات الويب.
- **Web browser open (إنهاء مستعرض الويب)**—حدد هذا الخيار لتقطيع كافة الأصول المرتبطة بالويب مثل سجل عنوان URL الخاص بالمستعرض عندما تقوم بغلق إحدى مستعرضات الويب.
- **Key sequence (تسلسل المفاتيح)**—حدد هذا الخيار لبدء استخدام إحدى تسلسلات المفاتيح.
- **Scheduler (المجدول)**—حدد مربع اختيار **Activate Scheduler (تنشيط المجدول)** ثم أدخل كلمة المرور الخاصة بنظام تشغيل Windows لديك ثم أدخل اليوم والساعة المراد تقطيع الأصول المحددة فيهما.

ملاحظة: يتم تقطيع ملف .dll وإزالته من النظام فقط إذا تم نقله إلى سلة المحذوفات.

٣. انقر فوق **Apply (تطبيق)**، ثم انقر فوق **OK (موافق)**.

تعيين جدول خاص بتبييض المساحة الحرة

ملاحظة: يستخدم تبييض المساحة الحرة للأصول التي تقوم بحذفها من خلال Windows Recycle Bin (سلة المحذوفات الموجودة في نظام تشغيل Windows) أو تلك التي تم حذفها يدويًا. لا يوفر تبييض المساحة الحرة أي أمن إضافي إلى الأصول التي تم تقطيعها.

لتعيين جدول خاص بتبييض المساحة الحرة:

١. افتح File Sanitizer (أداة تعقيم الملفات)، ثم انقر فوق **Free Space Bleaching** (تبييض المساحة الحرة).

٢. حدد مربع الاختيار **Activate Scheduler** (تنشيط المجدول)، ثم أدخل كلمة المرور الخاصة بنظام تشغيل Windows ثم أدخل التاريخ والساعة المراد تبييض القرص الصلب فيهما.

٣. انقر فوق **Apply (تطبيق)**، ثم انقر فوق **OK (موافق)**.

ملاحظة: يمكن أن تستغرق عملية تبييض المساحة الحرة وقتًا طويلاً. على الرغم من أنه يتم تنفيذ عملية تبييض المساحة الحرة في الخلفية، إلا إن ذلك سيؤدي إلى إبطاء أداء جهاز الكمبيوتر لديك نتيجة لحدوث زيادة في استخدام المعالج.

تحديد أو إنشاء إحدى ملفات تعريف التقطيع

يمكنك تحديد إحدى وسائل المسح واختيار الأصول المراد تقطيعها من خلال اختيار ملف تعريف محدد مسبقًا أو من خلال إنشاء ملف التعريف الخاص بك.

تحديد إحدى ملفات تعريف التقطيع المحددة مسبقًا

عندما تقوم باختيار إحدى ملفات تعريف التقطيع (High Security (أمن عالي)، أو Medium Security (أمن متوسط)، أو Low Security (أمن منخفض))، فإنه يتم تلقائيًا تحديد وسيلة مسح محددة مسبقًا وقائمة بالأصول. يمكنك النقر فوق زر **View Details (عرض التفاصيل)** لعرض قائمة الأصول المحددة مسبقًا والتي تم تحديدها للتقطيع.

لتحديد إحدى ملفات تعريف التقطيع المحددة مسبقًا:

١. قم بفتح File Sanitizer (أداة تعقيم الملفات)، ثم انقر فوق **Settings** (إعدادات).

٢. انقر فوق إحدى ملفات تعريف التقطيع المحددة مسبقًا.

٣. انقر فوق زر **View Details (عرض التفاصيل)** لعرض قائمة الأصول التي تم تحديدها للتقطيع.

٤. تحت **Shred the following (تقطيع التالي)**، حدد مربع الاختيار الموجود بجوار كل أصل والذي تريد التأكيد على تقطيعه.

٥. انقر فوق **Apply (تطبيق)**، ثم انقر فوق **OK (موافق)**.

تخصيص ملف تعريف للتقطيع

عندما تقوم بإنشاء إحدى ملفات تعريف التقطيع، قم بتحديد عدد دورات التقطيع والأصول التي سيتم تضمينها في التقطيع والأصول التي سيتم تأكيدها قبل التقطيع والأصول التي سيتم استبعادها من التقطيع:

١. قم بفتح File Sanitizer (أداة تعقيم الملفات) ثم انقر فوق **Settings (إعدادات)**، ثم انقر فوق **Advanced Security Settings (إعدادات الحماية المتقدمة)**، ثم فوق **View Details (عرض التفاصيل)**.

٢. حدد عدد دورات التقطيع.

ملاحظة: سيتم تنفيذ عدد دورات التقطيع المحدد في كل أصل. على سبيل المثال، إذا قمت باختيار 3 دورات، فسيتم تنفيذ خوارزمية تقوم بحجب البيانات في 3 مرات منفصلة. إذا قمت باختيار دورات التقطيع الأعلى في الأمن، فقد يستغرق التقطيع وقت كبير؛ على الرغم من ذلك كلما زاد عدد دورات التقطيع التي تقوم بتحديدها قل احتمال استعادة البيانات.

٣. حدد الأصول التي تريد تقطيعها:

أ. من **Available Shred Options** (خيارات التقطيع المتاحة)، انقر فوق إحدى الأصول، ثم انقر فوق **Add** (إضافة).

ب. لإضافة أصل مخصص انقر فوق **Add Custom Option (إضافة خيار مخصص)**، ثم قم باستعراض اسم الملف أو المجلد أو كتابة المسار الخاص به. انقر فوق **Open** (فتح)، ثم انقر فوق **OK** (موافق). من **Available Shred Options** (خيارات التقطيع المتاحة)، انقر فوق الأصل المخصص، ثم انقر فوق **Add** (إضافة).

ملاحظة: لإزالة أصل من خيارات التقطيع المتاحة, انقر فوق الأصل, ثم انقر فوق **Delete** (حذف).

٤. تحت **Shred the following (تقطيع التالي)**، حدد مربع الاختيار الموجود بجوار كل أصل والذي تريد التأكيد على تقطيعه

ملاحظة: لإزالة أصل من قائمة التقطيع، انقر فوق الأصل، ثم انقر فوق **Remove** (إزالة).

٥. لحماية الملفات أو المجلدات من التقطيع التلقائي, فمن **Do not shred the following** (عدم تقطيع ما يلي), انقر فوق **Add** (إضافة), ثم استعرض أو اكتر المسار المؤدي إلى اسم المف أو مجلده. انقر فوق **Open** (فتح)، ثم انقر فوق **OK** (موافق).

ملاحظة: لإزالة أصل من قائمة الاستبعاد، انقر فوق الأصل، ثم انقر فوق **Delete** (حذف).

٦. عندما تقوم بتكوين ملف تعريف التقطيع، انقر فوق **Apply (تطبيق)**، ثم انقر فوق **OK (موافق)**.

تخصيص حذف عادي لملف التعريف

يقوم الحذف العادي لملف التعريف بإجراء حذف عادي للأصول دون تقطيعها. عندما تقوم بتخصيص حذف عادي لملف التعريف، قم بتحديد الأصول التي سيتم تضمينها للحذف العادي والأصول التي سيتم تأكيدها قبل تنفيذ الحذف العادي والأصول التي سيتم استبعادها من الحذف العادي.

ملاحظة: إذا استخدمت خيار الحذف العادي، فيمكن تنفيذ تبييض المساحة الحرة أحيانًا على الأصول التي تم حذفها يدويًا أو بواسطة Recycle Bin (سلة المحذوفات) لـWindows.

لتخصيص حذف عادي لملف التعريف:

١. قم بفتح File Sanitizer (أداة تعقيم الملفات) ثم انقر فوق **Settings (إعدادات)**، ثم انقر فوق **Simple Delete Setting (إعدادات الحذف العادي)**، ثم فوق **View Details (عرض التفاصيل)**.

٢. حدد الأصول التي تريد حذفها:

أ. من **Available delete Options** (خيارات الحذف المتاحة)، انقر فوق إحدى الأصول، ثم انقر فوق **Add** (إضافة).

ب. لإضافة أصل مخصص **Add Custom Option (إضافة خيار مخصص)**، أدخل اسم الملف أو اسم المجلد ثم انقر فوق **OK (موافق)**. انقر فوق الأصل المخصص، ثم انقر فوق **Add (إضافة)**.

ملاحظة: لحذف إحدى الأصول من خيارات الحذف المتاحة، انقر فوق الأصل، ثم انقر فوق **Delete** (حذف).

٣. تحت **Delete the following (حذف التالي)**، حدد مربع الاختيار الموجود بجوار كل أصل والذي تريد التأكيد على حذفه.

ملاحظة: لإزالة أصل من قائمة الحذف، انقر فوق الأصل، ثم انقر فوق **Remove** (إزالة).

٤. تحت **Do not delete the following (لا تقم بحذف التالي)**، انقر فوق **Add (إضافة)** لتحديد الأصول المحددة التي تريد استبعادها من التقطيع.

ملاحظة: لإزالة أصل من قائمة الاستبعاد، انقر فوق الأصل، ثم انقر فوق **Delete** (حذف).

٥. عندما تقوم بتكوين حذف بسيط لملف التعريف، انقر فوق **Apply (تطبيق)**، ثم انقر فوق **OK (موافق)**.

مهام عامة

يمكنك استخدام File Sanitizer (أداة تعقيم الملفات) لإجراء المهام التالية:

- استخدام إحدى تسلسل المفاتيح لبدء التقطيع—تسمح لك هذه الميزة بإنشاء تسلسل مفاتيح (على سبيل المثال s+alt+ctrl) لبدء التقطيع. للمزيد من التفاصيل، راجع استخدام تسلسل المفاتيح لبدء التقطيع في صفحة ٦٧.
- استخدام رمز File Sanitizer (أداة تعقيم الملفات) لبدء التقطيع—تعد هذه الميزة مماثلة لميزة السحب والإسقاط الموجودة في نظام تشغيل Windows. للمزيد من التفاصيل، راجع استخدام رمز أداة تعقيم الملف في صفحة ٦٧.
- تقطيع أصل معين أو كافة الأصول المحددة يدويًا—تسمح لك هذه الميزات بتقطيع البنود يدويًا دون الانتظار إلى استدعاء جدول التقطيع الدوري. للمزيد من التفاصيل، راجع تقطيع إحدى الأصول يدويًا في صفحة ٦٨ أو تقطيع كافة العناصر المحددة يدويًا في صفحة ٦٨.
- تنشيط تبييض المساحة الحرة يدويًا—تسمح لك هذه الميزة بتنشيط تبييض المساحة الحرة يدويًا. للمزيد من التفاصيل، راجع تنشيط تبييض المساحة الحرة يدويًا في صفحة ٦٨.
- إلغاء عملية التقطيع أو تبييض المساحة الحرة—تسمح لك هذه الميزة بإيقاف عملية التقطيع أو تبييض المساحة الحرة. للمزيد من التفاصيل، راجع إلغاء عملية التقطيع أو تبييض المساحة الحرة في صفحة ٦٩.
- عرض ملفات السجل—تسمح لك هذه الميزة بعرض ملفات سجل التقطيع أو تبييض المساحة الحرة التي تحتوي على أي أخطاء أو فشل من أخر عملية تقطيع أو تبييض المساحة الحرة. للمزيد من التفاصيل، راجع عرض ملفات السجل في صفحة ٦٩.

ملاحظة: يمكن أن تستغرق عملية التقطيع أو تبييض المساحة الحرة وقتًا طويلاً. على الرغم من أنه يتم تنفيذ عملية التقطيع أو تبييض المساحة الحرة في الخلفية، إلا إن ذلك سيؤدي إلى إبطاء أداء جهاز الكمبيوتر لديك نتيجة لحدوث زيادة في استخدام المعالج.

استخدام تسلسل المفاتيح لبدء التقطيع

لتحديد إحدى تسلسلات المفاتيح، اتبع هذه الخطوات:

١. افتح File Sanitizer (أداة تعقيم الملفات), وانقر فوق **Shred** (تقطيع).

٢. حدد مربع الاختيار **Key sequence (تسلسل المفاتيح)**.

٣. أدخل إحدى الأحرف في المربع المتاح.

٤. اختر إما خانة الاختيار الخاصة بـ**CTRL** أو تلك الخاصة بـ**ALT**, ثم حدد خانة اختيار **SHIFT**.

على سبيل المثال لبدء التقطيع التلقائي باستخدام المفتاح s وshift+ctrl قم بإدخال حرف s في المربع ثم حدد خيارات **CTRL** و **SHIFT**.

ملاحظة: تأكد من تحديد تسلسل مفاتيح مختلف عن تسلسلات المفاتيح الأخرى التي قمت بتكوينها.

لبدء التقطيع باستخدام تسلسل المفاتيح:

١. اضغط باستمرار على مفتاح shift ومفتاح ctrl أو alt (أو أي تركيب قمت بتحديده) أثناء الضغط على الحرف الذي اخترته.

٢. عند ظهور مربع حوار التأكيد، انقر فوق **Yes** (نعم).

استخدام رمز أداة تعقيم الملف

△ **تنبيه:** لا يمكن استرجاع الأصول التي تم تقطيعها. يرجى مراعاة الحذر عند تحديد العناصر التي سيتم تقطيعها يدويًا.

١. قم بالانتقال إلى المستند أو المجلد الذي تريد تقطيعه.

٢. قم بسحب الملف إلى رمز File Sanitizer (أداة تعقيم الملفات) الموجود على سطح المكتب.

٣. عند ظهور مربع حوار التأكيد، انقر فوق **Yes** (نعم).

تقطيع إحدى الأصول يدويًا

△ **تنبيه:** لا يمكن استرجاع الأصول التي تم تقطيعها. يرجى مراعاة الحذر عند تحديد العناصر التي سيتم تقطيعها يدويًا.

١. انقر بزر الماوس الأيمن **فوق رمز HP ProtectTools** الموجود في منطقة الإعلام ، في أقصى يمين شريط المهام، ثم انقر فوق **File Sanitizer (أداة تعقيم الملفات)**، ثم فوق **Shred One (تقطيع إحدى الأصول)**.

٢. عندما يتم ظهور مربع حوار التأكيد، قم بالانتقال إلى الأصل الذي تريد تقطيعه، ثم انقر فوق **OK (موافق)**.

ملاحظة: يمكن أن يكون الأصل الذي تحدده عبارة عن ملف أو مجلد فردي.

٣. عند ظهور مربع حوار التأكيد، انقر فوق **Yes** (نعم).

– أو –

١. انقر بزر الماوس الأيمن فوق رمز **File Sanitizer (أداة تعقيم الملفات)** على سطح المكتب ثم انقر فوق **Shred One (تقطيع إحدى الأصول)**.

٢. عندما يتم ظهور مربع حوار التأكيد، قم بالانتقال إلى الأصل الذي تريد تقطيعه، ثم انقر فوق **OK (موافق)**.

٣. عند ظهور مربع حوار التأكيد، انقر فوق **Yes** (نعم).

– أو –

١. افتح File Sanitizer (أداة تعقيم الملفات), وانقر فوق **Shred** (تقطيع).

٢. انقر فوق زر **Browse (استعراض)**.

٣. عندما يتم ظهور مربع حوار التأكيد، قم بالانتقال إلى الأصل الذي تريد تقطيعه، ثم انقر فوق **OK (موافق)**.

٤. عند ظهور مربع حوار التأكيد، انقر فوق **Yes** (نعم).

تقطيع كافة العناصر المحددة يدويًا

١. انقر بزر الماوس الأيمن فوق رمز **HP ProtectTools** الموجود في منطقة الإعلام ، في أقصى يمين شريط المهام، ثم انقر فوق **File Sanitizer (أداة تعقيم الملفات)**، ثم فوق **Shred Now (التقطيع الآن)**.

٢. عند ظهور مربع حوار التأكيد، انقر فوق **Yes** (نعم).

– أو –

١. انقر بزر الماوس الأيمن فوق رمز **File Sanitizer (أداة تعقيم الملفات)** على سطح المكتب ثم انقر فوق **Shred Now (التقطيع الآن)**.

٢. عند ظهور مربع حوار التأكيد، انقر فوق **Yes** (نعم).

– أو –

١. افتح File Sanitizer (أداة تعقيم الملفات), وانقر فوق **Shred** (تقطيع).

٢. انقر فوق الزر **Shred Now** (التقطيع الآن).

٣. عند ظهور مربع حوار التأكيد، انقر فوق **Yes** (نعم).

تنشيط تبييض المساحة الحرة يدويًا

١. انقر بزر الماوس الأيمن فوق رمز **HP ProtectTools** الموجود في منطقة الإعلام ، في أقصى يمين شريط المهام، ثم انقر فوق **File Sanitizer (أداة تعقيم الملفات)**، ثم فوق **Bleach Now (التبييض الآن)**.

٢. عند ظهور مربع حوار التأكيد، انقر فوق **Yes** (نعم).

– أو –

١. افتح File Sanitizer (أداة تعقيم الملفات)، ثم انقر فوق **Free Space Bleaching** (تبييض المساحة الحرة).

٢. انقر فوق **Bleach Now (التبييض الآن)**.

٣. عند ظهور مربع حوار التأكيد، انقر فوق **Yes** (نعم).

إلغاء عملية التقطيع أو تبييض المساحة الحرة

عندما تكون إحدى عمليات التقطيع أو تبييض المساحة الحرة قيد التقدم، سيتم ظهور رسالة فوق رمز HP ProtectTools Security Manager (إدارة الحماية HP ProtectTools) في منطقة الإعلام. تقوم الرسالة بتوفير التفاصيل حول عملية التقطيع أو تبييض المساحة الحرة (التقدم بالنسبة المئوية) وتعطيك خيار إلغاء العملية.

لإلغاء العملية:

▲ انقر فوق الرسالة, ثم انقر فوق **Stop** (إيقاف) لإلغاء الاتصال.

عرض ملفات السجل

في كل مرة يتم فيها إجراء عملية التقطيع أو تبييض المساحة الحرة، يتم إنشاء ملفات سجل لأي أخطاء أو فشل تم حدوثها. يتم تحديث ملفات السجل طبقًا لأخر عملية تقطيع أو تبييض المساحة الحرة.

ملاحظة: لا تظهر الملفات التي تم تقطيعها أو تبييضها بنجاح في ملفات السجل.

يتم إنشاء ملف سجل لعمليات التقطيع وملف سجل آخر لعمليات تبييض المساحة الحرة. يوجد كلا ملفي السجل على القرص الصلب في:

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

١٠ Device Access Manager (إدارة الوصول إلى الأجهزة) لـHP ProtectTools (طرز مختارة فقط)

يستخدم مسؤولو نظام تشغيل Device Access Manager for HP ProtectTools Windows® (إدارة الوصول للأجهزة لـHP ProtectTools) للتحكم في الوصول إلى الأجهزة على أنظمة التشغيل والحماية ضد الوصول غير المصرح به:

- يتم إنشاء ملفات تعريف الأجهزة لكل مستخدم لتحديد الأجهزة المسموح الوصول إليها أو تلك الممنوع الوصول إليها.
- يتم تنظيم المستخدمين في مجموعات مثل مجموعة Device Administrator (مسؤول الأجهزة) المحددة مسبقًا أو يمكن تحديد المجموعات باستخدام خيار Computer Management (إدارة الكمبيوتر) في قسم Administrative Tools (الأدوات الإدارية) في Control Panel (لوحة التحكم).
- يمكن منح الوصول إلى الأجهزة أو منعه استنادًا إلى العضوية في المجموعات.
- للأجهزة من نوع محرك أقراص CD-ROM أو DVD، فإنه يمكن السماح بالوصول للقراءة والوصول للكتابة أو منعه بشكل منفصل.

كما يمكن السماح للمستخدمين المحدودين بقراءة سياسية التحكم في الوصول إلى الأجهزة والتعديل فيها.

إجراءات الإعداد

فتح Device Access Manager (إدارة الوصول إلى الأجهزة)

لفتح Device Access Manager (إدارة الوصول إلى الأجهزة)، اتبع الخطوات التالية:

١. انقر فوق **Start (ابدأ)**، ثم **All Programs (كافة البرامج)**، ثم **HP**، ثم انقر فوق **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**.

٢. في الجزء الأيسر، انقر فوق **Device Access Manager** (إدارة الوصول إلى الأجهزة).

تكوين الوصول إلى الأجهزة

تعرض Device Access Manager for HP ProtectTools (إدارة الوصول إلى الأجهزة لـHP ProtectTools) ثلاثة عروض:

- يستخدم عرض Simple Configuration (التكوين العادي) للسماح بالوصول إلى بعض فئات الأجهزة لأعضاء مجموعة Device Administrators (مسؤولو الأجهزة) أو منع الوصول إليها.
- يستخدم عرض Device Class Configuration (تكوين أنواع الأجهزة) للسماح بالوصول إلى بعض أنواع الأجهزة أو بعض الأجهزة المحددة لمستخدمين أو مجموعات معينة أو منعهم من الوصول إليها.
- يستخدم عرض User Access Settings (إعدادات وصول المستخدم) لتحديد المستخدمين الذين يمكنهم عرض معلومات حول Simple Configuration (التكوين العادي) أو Device Class Configuration (تكوين فئات الأجهزة) أو التعديل فيها.

مجموعة مسؤولي الأجهزة

عند تثبيت Device Access Manager (إدارة الوصول إلى الأجهزة)، يتم إنشاء مجموعة Device Administrators (مسؤولو الأجهزة).

يمكن لمسؤولي النظام تنفيذ سياسة عادية للتحكم في الوصول إلى الأجهزة من خلال منع الوصول إلى مجموعة من فئات الأجهزة إذا لم يتم تصنيف المستخدم كمستخدم موثوق به (بخصوص الوصول إلى الأجهزة). الطريقة التي يوصى بها للتمييز بين مستخدمي "الأجهزة الموثوق بهم" ومستخدمي "الأجهزة غير الموثوق بهم" هو جعل جميع مستخدمي الأجهزة الموثوق بهم أعضاء في مجموعة Device Administrators (مسؤولو الأجهزة). من ثم سيؤدي السماح إلى أعضاء مجموعة Device Administrators (مسؤولو الأجهزة) بالوصول إلى الأجهزة عبر عروض Simple Configuration (التكوين العادي) أو Device Class Configuration (تكوين فئات الأجهزة) إلى ضمان تمكن مستخدمي "الأجهزة الموثوق بهم" من الوصول التام إلى المجموعة المحددة من فئات الأجهزة.

ملاحظة: لا تؤدي إضافة المستخدم إلى مجموعة Device Administrators (مسؤولو الأجهزة) إلى السماح تلقائيًا للمستخدم بالوصول إلى الأجهزة. على الرغم من ذلك، فإنه يمكن استخدام عرض Simple Configuration (التكوين العادي) للسماح لمستخدمي "الأجهزة الموثوق بهم" بالوصول إلى مجموعة فئات الأجهزة المطلوبة.

لإضافة مستخدمين إلى مجموعة Device Administrators (مسؤولو الأجهزة)، اتبع الخطوات التالية:

- في نظام تشغيل Windows 7 أو Vista أو XP Professional استخدم بطاقة MMC العادية "Local Users and Groups" ("المستخدمون والمجموعات المحلية").
- في الإصدارات المنزلية من نظام تشغيل Windows 7 أو Vista® أو XP من حساب مميز، اكتب التالي في إطار موجه الأوامر:

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

تكوين عادي

يمكن للمسؤولين والمستخدمين المصرح لهم باستخدام عرض Simple Configuration (التكوين العادي) لتعديل الوصول إلى فئات الأجهزة التالية لكافة غير المسؤولين على الأجهزة:

ملاحظة: كي يتمكن المستخدم أو المجموعة من استخدام هذا العرض لقراءة المعلومات الخاصة بالوصول إلى الأجهزة، يجب منحهم وصول "للقراءة" في عرض **User Access Settings (إعدادات وصول المستخدم)**. كي يتمكن المستخدم أو المجموعة من استخدام هذا العرض لتعديل المعلومات الخاصة بالوصول إلى الأجهزة، يجب منحهم وصول "للتغيير" في عرض **User Access Settings (إعدادات وصول المستخدم)**.

- كافة الوسائط القابلة للنقل (الأقراص المرنة ومحركات الأقراص المحمولة USB إلخ.)
- كافة محركات أقراص DVD/الأقراص المضغوطة
- كافة المنافذ التسلسلية والمتوازية
- كافة أجهزة Bluetooth®
- كافة أجهزة الأشعة تحت الحمراء
- كافة أجهزة المودم
- كافة أجهزة PCMCIA
- كافة أجهزة 1394

للسماح بوصول كافة غير المسؤولين على الأجهزة إلى إحدى فئات الأجهزة أو منعهم من ذلك، اتبع الخطوات التالية:

١. في الجزء الأيسر من **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**، انقر فوق **Device Access Manager (إدارة الوصول إلى الأجهزة)**، ثم انقر فوق **Simple Configuration (التكوين العادي)**.

٢. في الجزء الأيمن من HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)، لمنع الوصول حدد مربع الاختيار لإحدى فئات الأجهزة أو لجهاز محدد. قم بإلغاء تحديد مربع الاختيار للسماح بالوصول إلى فئة ذلك الجهاز أو لجهاز محدد.

إذا ظهرت إحدى مربعات الاختيار باللون الرمادي، فهذا يعني أنه تم تغيير القيم التي تؤثر على سيناريو الوصول من داخل عرض Device Class Configuration (تكوين فئات الأجهزة). لإعادة تعيين القيم إلى الإعدادات العادية، انقر فوق مربع الاختيار لمسحه أو إعادة تعيينه ثم انقر فوق **Yes (نعم)** للتأكيد.

٣. انقر فوق رمز **Save** (حفظ).

ملاحظة: إذا لم يتم تشغيل الخدمة في الخلفية، سيتم ظهور مربع حوار يسألك عما إذا كنت تريد بدء تشغيل الخدمة. انقر فوق **Yes** (نعم).

٤. انقر فوق **OK (موافق)**.

بدء تشغيل الخدمة في الخلفية

قبل تطبيق ملفات تعريف الأجهزة، ستقوم HP ProtectTools Security Manager (إدارة الحماية لـHP ProtectTools) بفتح مربع حوار يسألك عما إذا كنت تريد أن تبدأ تشغيل خدمة HP ProtectTools Device Locking/Auditing (قفل/تدقيق الأجهزة لـHP ProtectTools) في الخلفية. انقر فوق **Yes** (نعم). سيتم بدأ تشغيل الخدمة في الخلفية ومنذ ذلك الحين فصاعدًا سيتم تشغيلها تلقائيًا متى يتم بدأ تشغيل النظام.

ملاحظة: يجب تحديد إحدى ملفات تعريف الأجهزة قبل عرض المطالبة الخاصة بتشغيل الخدمة في الخلفية.

كما يمكن للمسؤولين بدء تشغيل هذه الخدمة أو إيقافها:

١. انقر فوق **Start** (ابدأ)، ثم انقر فوق **Control Panel** (لوحة التحكم).

٢. انقر فوق **Administrative Tools (الأدوات الإدارية)**، ثم انقر فوق **Services (خدمات)**.

٣. قم بالبحث عن خدمة **HP ProtectTools Device Locking/Auditing (قفل/تدقيق الأجهزة لـHP ProtectTools)**.

لا يؤدي غلق خدمة Device Locking/Auditing (قفل/تدقيق الأجهزة) إلى إيقاف تشغيل قفل الجهاز. يتحكم عنصران في قفل الجهاز:

- خدمة Device Locking/Auditing (قفل/تدقيق الأجهزة)
- برنامج تشغيل DAMDrv.sys

يؤدي بدء تشغيل الخدمة إلى بدء تشغيل برنامج التشغيل الخاص بالجهاز لكن لا يؤدي إيقاف تشغيل الخدمة إلى إيقاف تشغيل برنامج التشغيل.

لتحديد ما إذا كانت الخدمة قيد التشغيل في الخلفية أم لا، قم بفتح إطار موجه الأوامر ثم اكتب sc query flcdlock.

لتحديد ما إذا كان برنامج التشغيل الخاص بالجهاز قيد التشغيل في الخلفية أم لا، قم بفتح إطار موجه الأوامر ثم اكتب sc query damdrv.

Device Class Configuration (تكوين فئة الأجهزة)

يمكن للمسؤولين والمستخدمين المصرح لهم عرض قوائم المستخدمين والمجموعات المسموح لها أو الممنوعة من الوصول إلى بعض فئات الأجهزة أو أجهزة محددة والتعديل في هذه القوائم.

ملاحظة: كي يتمكن المستخدم أو المجموعة من استخدام هذا العرض لقراءة المعلومات الخاصة بالوصول إلى الأجهزة، يجب منحهم وصول "للقراءة" في عرض **User Access Settings (إعدادات وصول المستخدم)**. كي يتمكن المستخدم أو المجموعة من استخدام هذا العرض لتعديل المعلومات الخاصة بالوصول إلى الأجهزة، يجب منحهم وصول "للتغيير" في عرض **User Access Settings (إعدادات وصول المستخدم)**.

يحتوي عرض تكوين فئة الجهاز على الأقسام التالية:

- **Device List (قائمة الأجهزة)**—تعرض كافة فئات الأجهزة والأجهزة المثبتة على النظام أو التي تم تثبيتها على النظام مسبقًا.
  - يتم تطبيق الحماية على فئات الأجهزة. سيتمكن المستخدم أو المجموعة المحددة من الوصول إلى أي جهاز في فئات الأجهزة.
  - كما يمكن تطبيق الحماية إلى الأجهزة المحددة.
- **User List (قائمة المستخدمين)**—تعرض كافة المستخدمين والمجموعات المسموح لها الوصول إلى فئات الأجهزة المحددة أو إلى جهاز معين أو الممنوعة من ذلك الوصول.
  - يمكن أن يكون إدخال User List (قائمة المستخدمين) مخصص لمستخدم معين أو لمجموعة ينتمي إليها المستخدم كعضو.
  - إذا كان هناك إدخال مستخدم أو مجموعة في User List (قائمة المستخدمين) غير متاح، فهذا يعني إنه قد تم اشتقاق الإعدادات من فئة الأجهزة الموجودة في Device List (قائمة الأجهزة) أو من Class folder (مجلد الفئات).
  - يمكن التحكم أيضًا في بعض فئات الأجهزة مثل DVD و CD-ROM من خلال السماح بالوصول بشكل منفصل لعمليات القراءة والكتابة أو منع ذلك الوصول.

    أما بشأن الأجهزة والفئات الأخرى، فإنه يمكن اشتقاق حقوق الوصول للقراءة والكتابة. على سبيل المثال، يمكن اشتقاق الوصول للقراءة من فئة أعلى لكن يمكن منع الوصول للكتابة على وجه التخصيص إلى مستخدم أو مجموعة.

ملاحظة: إذا كان مربع اختيار القراءة فارغ، فذلك يعني إنه لا يوجد تأثير لإدخال التحكم في الوصول على الوصول للقراءة إلى الجهاز. فإنه لا يقوم بالسماح بالوصول للقراءة إلى الجهاز أو منع ذلك الوصول.

مثال 1—إذا تم منع مستخدم أو مجموعة من الوصول للكتابة إلى إحدى الأجهزة أو فئة من الأجهزة:

يمكن منح نفس المستخدم أو المجموعة أو أي عضو في نفس المجموعة وصول للكتابة أو وصول للكتابة+للقراءة فقط لجهاز أقل من هذا الجهاز من حيث تسلسل الأجهزة.

مثال 2—إذا تم منح مستخدم أو مجموعة الوصول للكتابة إلى إحدى الأجهزة أو فئة من الأجهزة:

يمكن منع نفس المستخدم أو المجموعة أو أي عضو في نفس المجموعة من الوصول للكتابة أو وصول للكتابة+للقراءة فقط لنفس الجهاز أو لجهاز أقل من هذا الجهاز من حيث تسلسل الأجهزة.

مثال 3—إذا تم منح مستخدم أو مجموعة الوصول للقراءة إلى إحدى الأجهزة أو فئة من الأجهزة:

يمكن منع نفس المستخدم أو المجموعة أو أي عضو في نفس المجموعة من الوصول للقراءة أو وصول للكتابة+للقراءة فقط لنفس الجهاز أو لجهاز أقل من هذا الجهاز من حيث تسلسل الأجهزة.

مثال 4—إذا تم منع مستخدم أو مجموعة من الوصول للقراءة إلى إحدى الأجهزة أو فئة من الأجهزة:

يمكن منح نفس المستخدم أو المجموعة أو أي عضو في نفس المجموعة وصول للقراءة أو وصول للكتابة+للقراءة فقط لجهاز أقل من هذا الجهاز من حيث تسلسل الأجهزة.

مثال 5—إذا تم منح مستخدم أو مجموعة الوصول للقراءة+للكتابة إلى إحدى الأجهزة أو فئة من الأجهزة:

يمكن منع نفس المستخدم أو المجموعة أو أي عضو في نفس المجموعة من الوصول للكتابة أو وصول للكتابة+للقراءة فقط لنفس الجهاز أو لجهاز أقل من هذا الجهاز من حيث تسلسل الأجهزة.

مثال 6—إذا تم منع مستخدم أو مجموعة من الوصول للقراءة+للكتابة إلى إحدى الأجهزة أو فئة من الأجهزة:

يمكن منح نفس المستخدم أو المجموعة أو أي عضو في نفس المجموعة وصول للقراءة أو وصول للكتابة+للقراءة فقط لجهاز أقل من هذا الجهاز من حيث تسلسل الأجهزة.

منع وصول المستخدم أو المجموعة

لمنع وصول أحد المستخدمين أو إحدى المجموعات من الوصول إلى إحدى الأجهزة أو إحدى فئات الأجهزة، اتبع الخطوات التالية:

١. في الجزء الأيسر من **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**، انقر فوق **Device Access Manager (إدارة الوصول إلى الأجهزة)**، ثم انقر فوق **Device Class Configuration (تكوين فئات الأجهزة)**.

٢. في قائمة الأجهزة، انقر فوق فئة الأجهزة التي تريد تكوينها.

- فئة الأجهزة
- كافة الأجهزة
- جهاز فردي

٣. تحت **User/Groups (المستخدمين/المجموعات)**، انقر فوق المستخدم أو المجموعة المراد منعها من الوصول.

٤. انقر فوق **Deny (منع)** بجوار المستخدم أو المجموعة.

٥. انقر فوق رمز **Save** (حفظ).

ملاحظة: عندما يتم تعيين إعدادات منع الوصول أو السماح به على نفس مستوى الجهاز للمستخدم، فإن الأسبقية تكون لمنع الوصول عن منح الوصول.

منح الوصول إلى المستخدم أو المجموعة

لمنح أحد المستخدمين أو إحدى المجموعات إذن الوصول إلى إحدى الأجهزة أو إحدى فئات الأجهزة، اتبع الخطوات التالية:

١. في الجزء الأيسر من **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**، انقر فوق **Device Access Manager (إدارة الوصول إلى الأجهزة)**، ثم انقر فوق **Device Class Configuration (تكوين فئات الأجهزة)**.

٢. في قائمة الأجهزة، انقر فوق إحدى ما يلي:

- فئة الأجهزة
- كافة الأجهزة
- جهاز فردي

٣. انقر فوق **Add** (إضافة).

يتم ظهور مربع حوار **Select Users or Groups** (تحديد المستخدمين أو المجموعات).

٤. انقر فوق **Advanced** (متقدم), ثم انقر فوق **Find Now** (البحث الآن) للبحث عن مستخدمين أو مجموعات للإضافة.

٥. انقر فوق أحد المستخدمين أو إحدى المجموعات لإضافتها في قائمة المستخدمين والمجموعات المتاحة ثم انقر فوق **OK (موافق)**.

٦. انقر فوق **OK (موافق)** مرة أخرى.

٧. انقر فوق **Allow (السماح)** لمنح الوصول إلى هذا المستخدم أو هذه المجموعة.

٨. انقر فوق رمز **Save** (حفظ).

إزالة الوصول إلى المستخدم أو المجموعة

لإزالة إذن وصول أحد المستخدمين أو إحدى المجموعات إلى إحدى الأجهزة أو إحدى فئات الأجهزة، اتبع الخطوات التالية:

١. في الجزء الأيسر من **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**، انقر فوق **Device Access Manager (إدارة الوصول إلى الأجهزة)**، ثم انقر فوق **Device Class Configuration (تكوين فئات الأجهزة)**.

٢. في قائمة الأجهزة، انقر فوق فئة الأجهزة التي تريد تكوينها.

- فئة الأجهزة
- كافة الأجهزة
- جهاز فردي

٣. تحت **User/Groups (المستخدمين/المجموعات)**، انقر فوق المستخدم أو المجموعة التي تريد إزالتها ثم انقر فوق **Remove (إزالة)**.

٤. انقر فوق رمز **Save** (حفظ).

السماح بوصول أحد المستخدمين أو إحدى المجموعات إلى إحدى فئات الأجهزة

للسماح بوصول أحد المستخدمين إلى إحدى فئات الأجهزة مع منع وصول كافة الأعضاء الآخرين الذين ينتموا لمجموعة هذا المستخدم، اتبع الخطوات التالية:

١. في الجزء الأيسر من **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**، انقر فوق **Device Access Manager (إدارة الوصول إلى الأجهزة)**، ثم انقر فوق **Device Class Configuration (تكوين فئات الأجهزة)**.

٢. في قائمة الأجهزة، انقر فوق فئة الأجهزة التي تريد تكوينها.

- فئة الأجهزة
- كافة الأجهزة
- جهاز فردي

٣. تحت **User/Groups (المستخدمين/المجموعات)**، حدد المجموعة التي تريد منعها من الوصول ثم انقر فوق **Deny (منع)**.

٤. انتقل إلى المجلد الموجود أسفل الفئة المطلوبة ثم قم بإضافة المستخدم المحدد.

٥. انقر فوق **Allow (السماح)** لمنح الوصول إلى هذا المستخدم.

٦. انقر فوق رمز **Save** (حفظ).

السماح بوصول أحد المستخدمين أو إحدى المجموعات إلى جهاز معين

يمكن للمسؤولين السماح بوصول أحد المستخدمين إلى جهاز معين مع منع وصول كافة الأعضاء الآخرين الذين ينتموا لمجموعة هذا المستخدم، إلى كافة الأجهزة الموجودة في الفئة:

١. في الجزء الأيسر من **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**، انقر فوق **Device Access Manager (إدارة الوصول إلى الأجهزة)**، ثم انقر فوق **Device Class Configuration (تكوين فئات الأجهزة)**.

٢. في قائمة الأجهزة، انقر فوق فئة الأجهزة التي تريد تكوينها، ثم انتقل إلى المجلد الموجود أسفل هذه الفئة.

٣. انقر فوق **Add** (إضافة). يتم ظهور مربع حوار **Select Users or Groups** (تحديد المستخدمين أو المجموعات).

٤. انقر فوق **Advanced (متقدم)**، ثم انقر فوق **Find Now (البحث الآن)** للبحث عن مجموعة المستخدم التي سيتم منعها من الوصول إلى كافة الأجهزة الموجودة في الفئة.

٥. انقر فوق المجموعة، ثم انقر فوق **OK (موافق)**.

٦. انتقل إلى الجهاز المعين الموجود تحت فئة الأجهزة والذي سيتم السماح بوصول المستخدم إليه.

٧. انقر فوق **Add** (إضافة). يتم ظهور مربع حوار **Select Users or Groups** (تحديد المستخدمين أو المجموعات).

٨. انقر فوق **Advanced** (متقدم), ثم انقر فوق **Find Now** (البحث الآن) للبحث عن مستخدمين أو مجموعات للإضافة.

٩. انقر فوق المستخدم الذي سيتم السماح له بالوصول، ثم انقر فوق **OK (موافق)**.

١٠. انقر فوق **Allow (السماح)** لمنح الوصول إلى هذا المستخدم.

١١. انقر فوق رمز **Save** (حفظ).

إعادة تعيين التكوين

△ **تنبيه:** تؤدي إعادة تعيين التكوين إلى تجاهل كافة تغييرات التكوين التي تم إجراءها على الأجهزة واعادة الإعدادات إلى القيم التي تم تعيينها لدى الشركة المصنعة.

لإعادة إعدادات التكوين إلى القيم الخاصة بالشركة المصنعة، اتبع هذه الخطوات:

١. في الجزء الأيسر من **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**، انقر فوق **Device Access Manager (إدارة الوصول إلى الأجهزة)**، ثم انقر فوق **Device Class Configuration (تكوين فئات الأجهزة)**.

٢. انقر فوق زر **Reset (إعادة التعيين)**.

٣. انقر فوق **Yes** (نعم) للتأكيد.

٤. انقر فوق رمز **Save** (حفظ).

المهام المتقدمة

التحكم في الوصول إلى إعدادات التكوين

في عرض **User Access Settings (إعدادات وصول المستخدم)** يمكن للمسؤولين تحديد المجموعات أو المستخدمين المسموح لهم باستخدام صفحات Simple Configuration (التكوين البسيط) و Device Class Configuration (تكوين فئات الأجهزة).

ملاحظة: يجب أن يكون لدى المستخدم أو المجموعة "Full User Administrator rights" ("امتيازات مسؤول المستخدم الكاملة") للتمكن من التعديل في إعدادات عرض User Access Settings (إعدادات وصول المستخدم).

- يجب منح المستخدم أو المجموعة وصول "View (Read-only) Configuration Settings" (عرض (قراءة فقط) إعدادات التكوين) في User Access Settings (إعدادات وصول المستخدم) للتمكن من عرض البيانات الخاصة بـ Simple Configuration (التكوين البسيط) و Device Class Configuration (تكوين فئات الأجهزة).
- يجب منح المستخدم أو المجموعة وصول "Change Configuration Settings" ("تغيير إعدادات التكوين") في User Access Settings (إعدادات وصول المستخدم) للتمكن من تغيير البيانات الخاصة بـ Simple Configuration (التكوين البسيط) و Device Class Configuration (تكوين فئات الأجهزة).

ملاحظة: كما يجب منح أعضاء مجموعة Administrators (المسؤولين) وصول "للقراءة" كي يتمكنوا من عرض عروض Simple Configuration (التكوين البسيط) و Device Class Configuration (تكوين فئات الأجهزة) ووصول "للتغيير" كي يتمكنوا من تغيير البيانات باستخدام عروض Simple Configuration (التكوين البسيط) و Device Class Configuration (تكوين فئات الأجهزة).

ملاحظة: بعد تقييم مستويات الوصول لكافة المستخدمين والمجموعات، إذا لم يتم تحديد إما Allow (سماح) أو Deny (منع) لدى أحد المستخدمين في مستوى خاص من الوصول، فإن ذلك يعني أنه تم منع المستخدم من الوصول في ذلك المستوى.

منح الوصول إلى مجموعة أو مستخدم حالي

لمنح مجموعة أو مستخدم حالي الإذن بعرض إعدادات التكوين أو تغييرها، اتبع الخطوات التالية:

١. في الجزء الأيسر من **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**، انقر فوق **Device Access Manager (إدارة الوصول إلى الأجهزة)**، ثم انقر فوق **User Access Settings (إعدادات وصول المستخدم)**.

٢. انقر فوق إحدى المجموعات أو أحد المستخدمين لمنحه الوصول.

٣. تحت **Permissions (الأذونات)**، انقر فوق **Allow (السماح)** لكل نوع من الأذونات الذي سيتم منحه للمجموعة أو المستخدم المحدد:

ملاحظة: يتم منح الأذونات بشكل تراكمي. على سبيل المثال، إذا تم منح أحد المستخدمين "Change Configuration Settings," ("تغيير إعدادات التكوين،") فإنه يتم منحه إذن "View (Read-only) Configuration Settings" (عرض (قراءة فقط) إعدادات التكوين) تلقائيًا. يتم منح المستخدم الحاصل على "Full User Administrator Rights" ("امتيازات مسؤول المستخدم الكاملة") أذونات "Change Configuration Settings" ("تغيير إعدادات التكوين") و "View (Read-only) Configuration Settings" (عرض (قراءة فقط) إعدادات التكوين).

- Full User Administrator rights (امتيازات مسؤول المستخدم الكاملة)
- Change Configuration Settings (تغيير إعدادات التكوين)
- View (Read-only) Configuration Settings (عرض (قراءة فقط) إعدادات التكوين)

٤. انقر فوق رمز **Save** (حفظ).

منع الوصول إلى مجموعة أو مستخدم حالي

لمنع الإذن عن مجموعة أو مستخدم حالي من عرض إعدادات التكوين أو تغييرها، اتبع الخطوات التالية:

١. في الجزء الأيسر من **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**، انقر فوق **Device Access Manager (إدارة الوصول إلى الأجهزة)**، ثم انقر فوق **User Access Settings (إعدادات وصول المستخدم)**.

٢. انقر فوق إحدى المجموعات أو أحد المستخدمين لمنعه من الوصول.

٣. تحت **Permissions (الأذونات)**، انقر فوق **Deny (المنع)** لكل نوع من الأذونات الذي سيتم منعه للمجموعة أو المستخدم المحدد:

- Full User Administrator rights (امتيازات مسؤول المستخدم الكاملة)
- Change Configuration Settings (تغيير إعدادات التكوين)
- View (Read-only) Configuration Settings (عرض (قراءة فقط) إعدادات التكوين)

٤. انقر فوق رمز **Save** (حفظ).

إضافة مجموعة أو مستخدم جديد

لمنح مجموعة أو مستخدم جديد الإذن بعرض إعدادات التكوين أو تغييرها، اتبع الخطوات التالية:

١. في الجزء الأيسر من **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**، انقر فوق **Device Access Manager (إدارة الوصول إلى الأجهزة)**، ثم انقر فوق **User Access Settings (إعدادات وصول المستخدم)**.

٢. انقر فوق **Add** (إضافة). يتم ظهور مربع حوار **Select Users or Groups** (تحديد المستخدمين أو المجموعات).

٣. انقر فوق **Advanced** (متقدم), ثم انقر فوق **Find Now** (البحث الآن) للبحث عن مستخدمين أو مجموعات للإضافة.

٤. انقر فوق إحدى المجموعات أو أحد المستخدمين ثم انقر فوق **OK (موافق)**، ثم انقر مرة أخرى فوق **OK (موافق)**.

٥. انقر فوق **Allow (السماح)** لمنح الوصول إلى هذا المستخدم.

٦. انقر فوق رمز **Save** (حفظ).

إزالة وصول المجموعة أو المستخدم

لإزالة الإذن عن مجموعة أو مستخدم بعرض إعدادات التكوين أو تغييرها، اتبع الخطوات التالية:

١. في الجزء الأيسر من **HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)**، انقر فوق **Device Access Manager (إدارة الوصول إلى الأجهزة)**، ثم انقر فوق **User Access Settings (إعدادات وصول المستخدم)**.

٢. انقر فوق إحدى المجموعات أو أحد المستخدمين، ثم انقر فوق **Remove** (إزالة).

٣. انقر فوق رمز **Save** (حفظ).

وثائق ذات صلة

Device Access Manager for HP ProtectTools (إدارة الوصول إلى الأجهزة لـHP ProtectTools) متوافقة مع منتج HP ProtectTools Enterprise Device Access Manager المؤسسة (إدارة الوصول إلى الأجهزة الخاصة بشركة HP ProtectTools). عند العمل مع منتج المؤسسة ستسمح Device Access Manager for HP ProtectTools (إدارة الوصول إلى الأجهزة لـHP ProtectTools) بالوصول للقراءة فقط إلى الميزات الخاصة بها.

مزيد من المعلومات حول Device Access Manager for HP ProtectTools (إدارة الوصول إلى الأجهزة لـHP ProtectTools) متاحة على الويب على http://www.hp.com/hps/security/products.

١١ HP ProtectTools لـ LoJack Pro

يقوم برنامج Computrace LoJack Pro الذي يتم تشغيله بواسطة Absolute Software (الذي تم شراءه بشكل منفصل)، بمواجهة مشكلات أجهزة الكمبيوتر التي يتم فقدانها أو سرقتها بشكل متزايد.

يمكن تنشيط هذا البرنامج عميل Computrace الذي يظا نشطًا في جهاز الكمبيوتر لديك حتى في حالة إعادة تنسيق القرص الصلب أو استبداله.

يسمح برنامج LoJack Pro بمراقبة جهاز الكمبيوتر عن بعد وإدارته وتتبعه. إذا تم فقدان جهاز الكمبيوتر الخاص بك أو سرقته فسيقوم Absolute's Recovery Team (فريق الاسترجاع الخاص بشركة Absolute) بمساعدتك على استرجاعه.*

ملاحظة: *تعتمد هذه الميزة على المكان الجغرافي. يرجى الرجوع إلى اتفاقية الاشتراك لدى Absolute Software للتعرف على المزيد من التفاصيل.

١٢ حل المشكلات

HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools)

وصف موجز	تفاصيل	الحل
لن يتم إتاحة البطاقات الذكية ورموز USB في Security Manager (إدارة الحماية) إذا تم تثبيتها بعد تثبيت Security Manager (إدارة الحماية).	كي تتمكن من استخدام البطاقات الذكية ورموز USB في Security Manager (إدارة الحماية)، يجب تثبيت برامج الدعم (برامج التشغيل، موفرو PKCS#11، الخ) قبل تثبيت Security Manager (إدارة الحماية). إذا كانت Security Manager (إدارة الحماية) مثبتة بالفعل لديك، فقم باتباع الخطوات التالية بعد تثبيت برامج دعم البطاقة الذكية أو الرمز:	تسجيل الدخول إلى Password Manager (إدارة كلمة المرور) في HP ProtectTools Security Manager (إدارة الحماية لـHP ProtectTools)، انقر فوق **Password Manager (إدارة كلمة المرور)**، ثم انقر فوق **Credentials (بيانات الاعتماد)**، ثم انقر فوق **Smart Card (البطاقة الذكية)** قم بإعادة تشغيل جهاز الكمبيوتر عند مطالبتك بذلك.
تخلق بعض صفحات التطبيقات الأخطاء التي تمنع المستخدم من تنفيذ المهام أو إكمالها.	يتوقف بعض التطبيقات المستندة إلى الويب عن الأداء نظرًا لنموذج تعطيل الوظيفية الخاص بـSingle Sign On (تسجيل الدخول الموحد). على سبيل المثال, يشير الرمز **!** في مثلث أصفر والذي يرى في Internet Explorer, إلى حدوث خطأ.	لا يقوم Security Manager Single Sign On (تسجيل الدخول الفردي لإدارة الحماية) بدعم كافة واجهات الويب الخاصة بالبرامج. قم بتعطيل دعم Single Sign On (تسجيل الدخول الفردي) لصفحة الويب المحددة من خلال إيقاف تشغيل دعم Single Sign On (تسجيل دخول فردي). راجع الوثائق الكاملة عن Single Sign On (تسجيل الدخول الفردي) المتاحة في ملفات Help (التعليمات) الخاصة ببرنامج Security Manager (إدارة الحماية). إذا لم يمكن تعطيل Single Sign On (تسجيل دخول موحد) معين بالنسبة إلى تطبيق محدد, فاتصل بالدعم الفني لـHP واطلب الدعم من الدرجة الثالثة من خلال جهة الاتصال في HP Service.
لم يعرض الخيار **Browse for Virtual Token** (استعراض عملة ظاهرية) خلال عملية تسجيل الدخول.	لا يمكن للمستخدم نقل مكان الرموز الظاهرية المسجلة في Password Manager (إدارة كلمة المرور) لأنه قم تم إزالة خيار الاستعراض للتقليل من المخاطر الأمنية.	تمت إزالة خيار الاستعراض لكونه يتيح لغير المستخدمين حذف الملفات وإعادة تسميتها والتحكم في Windows.
لا يتمكنون مسؤولو المجالات من تغيير كلمة مرور Windows حتى بعد المصادقة.	ذلك يحدث بعد قيام إحدى مسؤولي المجال بتسجيل الدخول إلى المجال وتسجيل هوية المجال من خلال Password Manager (إدارة كلمة المرور) مستخدمًا إحدى الحسابات التي تمتلك 'امتيازات المسؤول في المجال والكمبيوتر المحلي. عندما يحاول مسؤول المجال تغيير كلمة المرور الخاصة بنظام تشغيل Windows من Password Manager (إدارة كلمة المرور)، فستظهر للمسؤول رسالة خطأ في فشل تسجيل الدخول: **User account restriction (حساب المستخدم محدد)**.	لا تتمكن Password Manager (إدارة كلمة المرور) من تغيير كلمات مرور 'حسابات مستخدمي المجالات من خلال **تغيير كلمة المرور الخاصة بنظام تشغيل Windows**. تتمكن Security Manager (إدارة الحماية) من تغيير كلمات المرور الخاصة بالكمبيوتر المحلي فقط. يتمكن مستخدمو المجالات من تغيير كلمات مرورهم من خلال الخيار **Change password** (تغيير كلمة المرور) في **Windows Security** (أمان Windows), ولكنه لعدم حوزة مستخدم المجال على حساب فعلي في الكمبيوتر المحلي, لن يقدر Password Manager (إدارة كلمة المرور) سوى على تغيير كلمة المرور المستخدمة لتسجيل الدخول.
تواجه Password Manager (إدارة كلمة المرور) مشكلات تتعلق بعدم التوافق مع كلمة المرور "GINA" الخاصة بـCorel WordPerfect 12.	إذا قام المستخدم بتسجيل الدخول على Password Manager (إدارة كلمة المرور) وإنشاء مستند في WordPerfect وحفظه مع استخدام كلمة مرور للحماية، فإن Password Manager (إدارة كلمة المرور) لن تتمكن من اكتشاف كلمة المرور "GINA" أو التعرف عليها يدويًا أو تلقائيًا.	تبحث HP عن طرق تجنبية لتحسين المنتج في المستقبل.

وصف موجز	تفاصيل	الحل
لا تقوم Password Manager (إدارة كلمة المرور) بالتعرف على زر **Connect (الاتصال)** الموجود على الشاشة.	إذا تم ضبط اعتمادات Single Sign On (تسجيل الدخول الموحد) او Remote Desktop Connection (الاتصال بسطح المكتب البعيد) (RDP) إلى **Connect** (الاتصال), فعند تشغيل Single Sign On (تسجيل الدخول الموحد) ثانية, يدخل **Save As** (حفظ باسم) بدلاً من **Connect** (اتصال).	تبحث HP عن طرق تجنبية لتحسين المنتج في المستقبل.
لن يتمكن المستخدم من تسجيل الدخول في Password Manager (إدارة كلمة المرور) بعد الانتقال من وضع السكون إلى وضع الإسبات في نظام تشغيل Windows XP Service Pack 1 فقط.	بعد السماح للنظام بالانتقال إلى وضعي الإسبات والسكون، لن يتمكن المسؤول أو المستخدم من تسجيل الدخول في Password Manager (إدارة كلمة المرور) وسيستمر عرض شاشة تسجيل الدخول في نظام تشغيل Windows بغض النظر عن بيانات الاعتماد الخاصة بالتسجيل (كلمة المرور، أو بصمة الإصبع، أو بطاقة Java) التي تم تحديدها.	حدّث Windows إلى Service Pack 2 من خلال Windows Update (تحديث Windows). راجع المقال 813301 في قاعدة المعرفة لـMicrosoft في http://www.microsoft.com للاطلاع على المزيد من المعلومات بخصوص مصدر المشكلة. كي يتمكن المستخدم من تسجيل الدخول، يجب عليه تحديد Password Manager (إدارة كلمة المرور) ثم تسجيل الدخول. بعد تسجيل الدخول في Password Manager (إدارة كلمة المرور)، سيتم مطالبة المستخدم بتسجيل الدخول في نظام تشغيل Windows (يجب على المستخدم تحديد خيار تسجيل الدخول في نظام تشغيل Windows) لاستكمال عملية تسجيل الدخول. إذا قام المستخدم بتسجيل الدخول أولاً في نظام تشغيل Windows، فسيجب عليه تسجيل الدخول في Password Manager (إدارة كلمة المرور) يدويًا.
يفقد إجراء الحماية **Restore Identity** (استعادة الهوية) الاقتران بالعملة الظاهرية.	عندما يقوم المستخدم باستعادة الهوية، قد تفقد Password Manager (إدارة كلمة المرور) الاقتران مع مكان الرمز الظاهري في شاشة تسجيل الدخول. حتى في حالة تسجيل الرمزالظاهري في Password Manager (إدارة كلمة المرور)، سيجب على المستخدم إعادة تسجيل الرمز لاستعادة الاقتران.	يتم تصميم ذلك حاليًا. عند إلغاء تثبيت Security Manager (إدارة الحماية) دون الحفاظ على الهويات، سيتم تدمير جزء الرمز الخاص بالنظام (الخادم)، من ثم لن يكون من الممكن استخدام الرمز بعد الآن لتسجيل الدخول حتى إذا تم استعادة جزء الرمز الخاص بالعميل من خلال استعادة الهوية. تدرس HP خيارات طويلة الأمد لحل ذلك.

Device Access Manager for HP ProtectTools (إدارة الوصول إلى الأجهزة لـHP ProtectTools)

لقد تم منع وصول المستخدمين إلى الأجهزة داخل Device Access Manager (إدارة الوصول إلى الأجهزة) إلا أنه لا يزال من الممكن الوصول إلى الأجهزة.

- **Explanation (التوضيح)**—لقد تم استخدام Simple Configuration (التكوين البسيط) و/أو Device Class Configuration (تكوين فئات الأجهزة) داخل Device Access Manager (إدارة الوصول إلى الأجهزة) لمنع وصول المستخدمين إلى الأجهزة. على الرغم من منع المستخدمين من الوصول إلا إنه لا يزال بإمكانهم الوصول إلى الأجهزة.
- **الحل:**
  - تحقق من بدء تشغيل خدمة HP ProtectTools Device Locking/Auditing (قفل/تدقيق الأجهزة لـHP ProtectTools).
  - باعتبارك مستخدم إداري انقر فوق **Control Panel (لوحة التحكم)**، ثم انقر فوق **System and Maintenance (النظام والصيانة)**. في إطار Administrative Tools (الأدوات الإدارية) انقر فوق **Services (الخدمات)**، ثم قم بالبحث عن خدمة **HP ProtectTools Device Locking/Auditing (قفل/تدقيق الأجهزة لـHP ProtectTools)**. تحقق من بدء تشغيل الخدمة ومن أن نوع البدء هو **Automatic (تلقائي)**

تم وصول إحدى المستخدمين بشكل غير متوقع لإحدى الأجهزة أو تم منع وصول إحدى المستخدمين بشكل غير متوقع لإحدى الأجهزة.

- **Explanation (التوضيح)**—تم استخدام Device Access Manager (إدارة الوصول إلى الأجهزة) لمنع وصول المستخدمين لبعض الأجهزة والسماح لهم بالوصول إلى أجهزة أخرى. عندما يقوم المستخدم باستخدام النظام، فإنه سيمكنه الوصول إلى الأجهزة التي يعتقد قيام Device Access Manager (إدارة الوصول إلى الأجهزة) بمنعه من الوصول إليها وسيتم منعه من الوصول للأجهزة التي يعتقد قيام Device Access Manager (إدارة الوصول إلى الأجهزة) بالسماح له بالوصول إليها.
- **الحل:**
  - استخدم Device Class Configuration (تكوين فئات الأجهزة) داخل Device Access Manager (إدارة الوصول إلى الأجهزة) للاستقصاء عن'إعدادات أجهزة المستخدم.
  - انقر فوق **Security Manager (إدارة الحماية)**، ثم فوق **Device Access Manager (إدارة الوصول إلى الأجهزة)**، ثم انقر فوق **Device Class Configuration (تكوين فئات الأجهزة)**. قم بتوسيع المستويات في شجرة Device Class (فئة الأجهزة) ومراجعة الإعدادات القابلة للتطبيق لهذا المستخدم. قم بالتحقق من وجود أي أذونات "Deny" ("منع") يكون قد تم تعيينها إلى المستخدم أو أي من Windows Group (مجموعة نظام تشغيل Windows) التي قد يكون المستخدم عضوًا بها، على سبيل المثال المستخدمون، المسؤولون.

السماح أو المنع—لأي منهما الأسبقية؟

- **Explanation (التوضيح)**—داخل Device Class Configuration (تكوين فئات الأجهزة)، تم تعيين التكوين التالي:.
  - تم منح الإذن Allow (سماح) لمجموعة Windows (مثل BUILTIN\Administrators) بينما تم تخصيص الإذن Deny (رفض) لمجموعة Windows أخرى (مثل BUILTIN\Users) ذات المستوى عينه في تنظيم فئات الأجهزة الهيكلي (مثل DVD/CD-ROM Drives (محركات الأقراص المضغوطة وDVD).
  - إذا كان المستخدم عضوًا في تلك المجموعتين (على سبيل المثال المسؤولين)، أي منهما له الأسبقية؟
- **الحل:**
  - تم منع وصول المستخدم إلى الجهاز. تكون الأسبقية لـDeny (المنع) عن Allow (السماح).
  - لقد تم منع الوصول بسبب الطريقة التي يقوم نظام تشغيل Windows من خلالها باستنباط الأذن الفعال للجهاز. لقد تم منع مجموعة والسماح لمجموعة أخرى ولكن المستخدم عضو في المجموعتين. تم منع المستخدم لأن الأسبقية تكون لمنع الوصول عن السماح بالوصول.

- هناك حل بديل وهو منع مجموعة المستخدمين عند مستوى محركات أقراص DVD/CD-ROM والسماح إلى مجموعة المسؤولين عند المستوى الأقل من محركات أقراص DVD/CD-ROM.
- هناك حل بديل آخر وهو إنشاء مجموعات محددة خاصة بنظام تشغيل Windows، تكون إحداها لسماح الوصول إلى DVD/CD والآخرى لمنع الوصول إلى DVD/CD. سيتم إضافة المستخدمين المحددين إلى المجموعة المناسبة.

لقد تم استخدام عرض Simple Configuration (التكوين البسيط) لتحديد إحدى سياسات التحكم في الوصول إلى الأجهزة إلا أن المستخدمين الإداريين لا يمكنهم الوصول إلى الأجهزة.

- **Explanation (التوضيح)**—يقوم Simple Configuration (التكوين البسيط) بمنع وصول Users and Guests (المستخدمين والضيوف) والسماح بوصول Device Administrators (مسؤولو الأجهزة).
- **الحل:** قم بإضافة المستخدم الإداري إلى مجموعة Device Administrators (مسؤولو الأجهزة).

متفرقات

البرنامج المتأثر—وصف وجيز	تفاصيل	الحل
Security Manager (إدارة الحماية)—استقبل تحذير: **The security application can not be installed until the HP Protect Tools Security Manager is installed** (لا يمكن تثبيت تطبيق الحماية إلى أن يثبت HP Protect Tools Security Manager).	جميع تطبيقات الأمن مثل Java Card Security (أمن بطاقة Java) وتطبيقات القياس الحيوي هي عبارة عن أدوات إضافية لواجهة Security Manager (إدارة الحماية). يجب تثبيت Security Manager (إدارة الحماية) قبل تحميل أي أداة إضافية خاصة بالأمن معتمدة من HP.	يجب تثبيت البرنامج Security Manager (إدارة الحماية) قبل أن يمكن تثبيت أية إضافة حماية.
HP ProtectTools Security Manager (إدارة الحماية لـ HP ProtectTools)—أحيانًا, يُرجع خطأ عند إغلاق واجهة Security Manager (إدارة الحماية).	أحيانًا (1 من 12 واقعًا), يُخلق خطأ من خلال استخدام زر الإغلاق أعلى يمين الشاشة لإغلاق Security Manager (إدارة الحماية) قبل إتمام تحميل كافة التطبيقات الإضافية.	يتعلق ذلك بتبعية للتوقيت تخص وقت تحميل خدمات للإضافات عند إغلاق Security Manager (إدارة الحماية) وإعادة تشغيلها. نظرًا لكون PTHOST.exe وعاءً يضيف كافة التطبيقات الأخرى (الإضافات), فإنه يعتمد على إمكانية الإضافة من إتمام وقت تحميله (الخدمات). إن السبب الأساسي يعود إلى إغلاق الوعاء قبل إتاحة الوقت الكافي لإتمام تحميل الإضافة. اسمح لـSecurity Manager (إدارة الحماية) بإكمال الرسالة الخاصة بتحميل الخدمات (ترى أعلى نافذة Security Manager (إدارة الحماية)) مع كافة الإضافات المسرودة في العمود اليساري. لتجنب الفشل, أتح الوقت الكافي لتحميل هذه الإضافات.
HP ProtectTools—يجسد الوصول بلا حدود أو صلاحيات المسؤول غير المتحكم فيها خطرًا على الأمان.	ثمة العديد من المخاطر في الوصول غير المحدود إلى الكمبيوتر العميل من بينها: • حذف PSD • التعديل البشع في إعدادات المستخدم • تعطيل سياسات الحماية ووظائفها	يوصى بأن يقوم المسؤولون باتباع "أفضل الممارسات" في تقييد امتيازات المستخدم النهائي وتقييد وصول المستخدمين. لا يجب منح المستخدمين غير المخولين امتيازات إدارية.

مسرد المصطلحات

ATM Automatic Technology Manager (إدارة التقنيات التلقائية), التي تسمح للمسؤولين عن الشبكات بإدارة الأنظمة عن بعد في مستوى الـBIOS.

Drive Encryption (تشفير محركات الأقراص) تقوم بحماية البيانات الخاصة بك من خلال تشفير القرص الصلب مع جعل المعلومات غير قابلة للقراءة للأشخاص غير المخولين.

DriveLock تتطلب ميزات الحماية التي تربط محرك الأقراص إلى المستخدم أن يكتب المستخدم كلمة المرور الخاصة بـDriveLock عند تشغيل الكمبيوتر.

HP SpareKey عبارة عن نسخة من مفتاح تشفير محركات الأقراص.

Live Messenger History Viewer (عارض سجل برنامج Live Messenger) عبارة عن مكون خاص بالمحادثة يتبع لـPrivacy Manager (إدارة الخصوصية) يتيح لك البحث عن جلسات سجل المحادثة المشفرة وعرضها.

PKI قياس Public Key Infrastructure (بنية تحتية للمفتاح العام) الذي يعرف واجهات إنشاء واستخدام وإدارة الشهادات ومفاتيح التشفير.

PSD Personal secure drive (محرك أقراص شخصي آمن), الذي يوفر مساحة تخزين محمية للمعلومات الحساسة.

TXT مختصر Trusted Execution Technology (تكنولوجيا التشغيل الموثوق به).

Windows Logon Security (أمن تسجيل الدخول في نظام تشغيل Windows) يقوم بحماية حساب (حسابات) نظام تشغيل Windows الخاص بك من خلال المطالبة باستخدام بيانات اعتماد معينة للوصول.

أرشيف الاستعادة في حالات الطوارئ عبارة عن منطقة تخزين محمية تتيح إعادة تشفير مفاتيح المستخدم الأساسية من مفتاح واحد لمالك نظام أساسي ما إلى الآخر.

أساليب تسجيل الدخول الآمن عبارة عن الأسلوب المستخدم لتسجيل الدخول إلى الكمبيوتر.

أصل عبارة عن مكون يخص البيانات ويتكون من معلومات أو ملفات شخصية, بيانات السجل وبيانات تخص الويب, وما إلى ذلك, فتخزن هذه البيانات على محرك القرص الثابت.

إعادة التمهيد إجراء إعادة تشغيل الكمبيوتر.

اتصال مراسلة فورية آمن عبارة عن جلسة اتصالات تُرسَل خلالها الرسائل الموثوق بها من مرسل موثوق به إلى جهة اتصال موثوق بها.

استعادة عملية يتم من خلالها نسخ بيانات البرنامج من ملف نسخ احتياطي تم حفظه مسبقًا في هذا البرنامج.

البطاقة الذكية Smart card عبارة عن جهاز صغير, يشبه بطاقات الاعتماد حجمًا وشكلاً, ويخزن معلومات عن هوية صاحبه. وتستخدم هذه البطاقة للمصادقة على صاحبها أمام أجهزة الكمبيوتر.

الخدمة في الخلفية خدمة تشغيل HP ProtectTools Device Locking/Auditing (قفل/تدقيق الأجهزة لـHP ProtectTools) في الخلفية والتي يجب تشغيلها لتطبيق سياسات التحكم في الوصول إلى الأجهزة. يمكن عرضها من تطبيق Services (الخدمات) الموجود في خيار Administrative Tools (الأدوات الإدارية) في Control Panel (لوحة التحكم). إذا لم تكن الخدمة قيد التشغيل، فإن HP ProtectTools Security Manager (إدارة أمن HP ProtectTools) ستحاول بدء تشغيلها عندما يتم تطبيق سياسات التحكم في الوصول إلى الأجهزة.

المجموعة مجموعة من المستخدمين لديهم نفس مستوى الوصول أو منع الوصول إلى إحدى فئات الأجهزة أو إلى جهاز محدد.

المصادقة عند التشغيل عبارة عن ميزة حماية تتطلب المصادقة بشكل ما مثل بطاقة Java, رقاقة حماية, أو كلمة مرور, وذلك عند تشغيل الكمبيوتر.

النسخ الاحتياطي استخدام ميزة النسخ الاحتياطي لحفظ نسخة من بيانات البرامج الهامة في مكان خارج البرامج. من ثم يمكن استخدامها لاستعادة البيانات في وقت لاحق على نفس الكمبيوتر أو على كمبيوتر آخر.

بصمة الإصبع استخلاص رقمي لصورة بصمة الإصبع الخاصة بك. لا تقوم Security Manager (إدارة الحماية) أبدًا بتخزين صورة بصمة الإصبع الفعلية الخاصة بك.

بطاقة Java عبارة عن بطاقة قابلة للإزالة تُدخَل في الكمبيوتر. وتحتوي هذه البطاقة على معلومات هامة تخص تسجيل الدخول. يتطلب تسجيل الدخول باستخدام بطاقة Java في شاشة تسجيل الدخول الخاصة بـDrive Encryption (تشفير محركات الأقراص) إدخال بطاقة Java وكتابة اسم المستخدم والـPIN الخاص ببطاقة Java.

بطاقة المعرف أداة موجودة في الشريط الجانبي من نظام تشغيل Windows تستخدم في تعريف سطح المكتب الخاص بك بشكل مرئي من خلال اسم المستخدم الخاص بك والصورة التي تختارها. انقر فوق بطاقة المعرف لفتح HP ProtectTools Administrative Console (وحدة التحكم الإدارية لـHP ProtectTools)

تبييض المساحة الحرة عبارة عن الكتابة الآمنة على أصول محذوفة لتشويش محتوى الأصل المحذوف.

ترحيل عبارة عن مهمة تتيح إدارة شهادات Privacy Manager (إدارة الخصوصية) وجهات اتصالها الموثوق بها كما يتيح استعادتها ونقلها.

تسجيل الدخول كائن موجود داخل Security Manager (إدارة الحماية) يتألف من اسم مستخدم وكلمة مرور (مع إمكانية تحديد بيانات أخرى) ويستخدم لتسجيل الدخول في مواقع الويب والبرامج الأخرى.

تسجيل دخول موحد ميزة تقوم بحفظ بيانات المصادقة وتتيح لك استخدام Security Manager (إدارة الحماية) للوصول إلى الإنترنت وتطبيقات نظام تشغيل Windows التي تطلب المصادقة بواسطة كلمة مرور.

تشفير عبارة عن إجراء تشفير وإلغاء تشفير البيانات حيث يمكن حل شفرتها علي يدي أشخاص معينة فقط.

تشفير عبارة عن إجراء, كاستخدام الخوارزميات, يستعمل في مجال التكويد لتحويل نص عادي إلى نص مكوَّد بغرض منع المستقبلين غير المصرح بهم من قراءة هذه البيانات. ثمة العديد من أنواع تشفير البيانات, فإنها تعد أسس حماية الشبكات. وتشمل الأنواع الشائعة Data Encryption Standard (قياس تشفير البيانات) وتشفير المفتاح العام.

تقطيع عبارة عن تنفيذ خوارزمية تخفي البيانات المضمنة في أصل ما.

تقطيع تلقائي التقطيع المجدول الذي يقوم المستخدم بتعيينه في File Sanitizer (أداة تعقيم الملفات).

تقطيع يدوي عبارة عن التقطيع الفوري لأصل أو لمجموعة أصول, والذي يتجنب التقطيع المجدول التلقائي.

تنشيط المهام التي يجب اتمامها قبل إمكانية الوصول إلى أي من ميزات Drive Encryption (تشفير محرك الأقراص). يتم تنشيط Drive Encryption (تشفير محرك الأقراص) من خلال HP ProtectTools Setup Wizard (معالج إعداد HP ProtectTools). يمكن فقط للمسؤولين تنشيط Drive Encryption (تشفير محرك الأقراص). تتألف عملية التنشيط من كلٍ من تنشيط البرنامج وتشفير المحرك وإنشاء حساب للمستخدم وإنشاء مفتاح لتشفير النسخ الاحتياطي الأولي على جهاز تخزين قابل للنقل.

توقيع رقمي عبارة عن البيانات المرسلة مع الملفات والتي تتحقق من مرسل المادة, ومن أنه لم يتغير الملف بعد التوقيع عليه.

جلسة سجل المحادثات عبارة عن ملف مشفر يحتوي على سجل للجهتين المشتركتين في جلسة محادثة.

جهة اتصال مستقبلة موثوق بها عبارة عن شخص تلقى دعوة تخص تعيينه جهة اتصال موثوق بها.

جهة اتصال موثوق بها عبارة عن شخص تلقى دعوة خاصة بجهات الاتصال الموثوق بها.

حذف بسيط عبارة عن حذف مرجع Windows لأصل ما. ويبقى محتوى الأصل على محرك القرص الثابت إلى أن تتم كتابة البيانات المُخفية فوقه من خلال 'تقصير المساحة الفارغة'.

حساب شبكة عبارة عن حساب لمستخدم أو مسؤول في Windows, ويوجد هذا الحساب إما في كمبيوتر محلي, في مجموعة عمل, أو في مجال.

حساب مستخدم Windows عبارة عن ملف تعريف لشخص خُوِّل تسجيل الدخول إلى الشبكة أو الكمبيوتر الفردي.

حل الشفرة عبارة عن إجراء يتم استخدامه في نطاق علم التشفير لتحويل البيانات المشفرة إلى نص عادي.

ختم لجهات الاتصال الموثوق بها مهمة تضيف ختمًا رقميًا وتشفر الرسائل الإلكترونية وترسلها بعد المصادقة عليك باستخدام أسلوب تسجيل الدخول المحمي الذي حددته.

دعوة جهة اتصال موثوق بها عبارة عن رسالة إلكترونية ترسل إلى شخص ما, داعية إياه ليصبح 'جهة اتصال موثوق بها'.

دورة التقطيع عبارة عن عدد المرات التي تنفذ خوارزمية التقطيع فيها بالنسبة لكل أصل. أعلى ما كان عدد دورات التقطيع التي تحددها, آمن ما كان الكمبيوتر.

رسالة آمنة عبارة عن جلسة اتصالات تُرسَل خلالها الرسائل الموثوق بها من مرسل موثوق به إلى جهة اتصال موثوق بها.

زر Send Security (الإرسال الآمن) زر برمجي يتم عرضه في شريط أدوات رسائل Microsoft Outlook الإلكترونية الصادرة. يسمحك النقر فوق هذا الزر بالتوقيع على رسائل Microsoft Outlook الإلكترونية و/أو بتشفيرها.

زر Sign and Encrypt (التوقيع والتشفير) زر برمجي يتم عرضه في شريط أدوات تطبيقات Microsoft Outlook. يسمحك النقر فوق هذا الزر بالتوقيع على مستند لـMicrosoft Outlook أو بتشفيره أو حل شفرته.

سطر التوقيع عبارة عن عنصر نائب عن عرض التوقيع الرقمي المرئي. بعد التوقيع على المستندات, يظهر اسم الموقع وطريقة المصادقة. كما يمكن تضمين تأريخ التوقيع ولقب الموقع.

سلسلة مفاتيح عبارة عن تركيب لمفاتيح معينة يشغل الضغط عليها التقطيع التلقائي—على سبيل المثال, s+alt+ctrl.

سلطة الشهادات عبارة عن خدمة تصدر الشهادات المطلوبة لتشغيل بنية أساسية خاصة بمفتاح عمومي.

سياسة التحكم في الوصول إلى الأجهزة قائمة الأجهزة التي يكون المستخدم مسموح بالوصول إليها أو ممنوع من ذلك الوصول.

شاشة تسجيل الدخول إلى Drive Encryption عبارة عن شاشة تخص تسجيل الدخول والتي يتم عرضها قبل تشغيل Windows. وعلى المستخدمين أن يدخلوا اسم المستخدم وكلمة المرور الخاصة بـWindows أو الـPIN الخاص بـبطاقة Java. ففي معظم الظروف, يؤدي إدخال المعلومات الصحيحة في شاشة تسجيل الدخول الخاصة بـDrive Encryption (تشفير محركات الأقراص) إلى الوصول إلى Windows مباشرة دون ضرورة تسجيل الدخول ثانية في شاشة تسجيل الدخول الخاصة بـWindows.

شهادة Privacy Manager (إدارة الخصوصية) عبارة عن شهادة رقمية تتطلب المصادقة كل مرة تستخدمها لعمليات التشفير, مثل التوقيع على رسائل البريد الإلكتروني ومستندات Microsoft Office وتشفيرها.

شهادة رقمية عبارة عن اعتمادات تثبت هوية فرد أو شركة ما وذلك من خلال ربط هوية مالك الشهادة الرقمية بمفتاحين إلكترونيين يستخدمان للتوقيع على المعلومات الرقمية.

عملة راجع أسلوب تسجيل الدخول الآمن

عملة USB عبارة عن جهاز حماية يخزن معلومات تُعرِّف المستخدم. ويتم استخدام هذا الجهاز مثل بطاقة Java أو قارئ بيولوجي, للمصادقة على المستخدم أمام الكمبيوتر.

عملة ظاهرية ميزة تخص الحماية يشبه عملها عمل بطاقات Java وقراء البطاقات. ويتم حفظ العملة إما في محرك القرص الثابت في الكمبيوتر أو في سجل Windows. عند تسجيل دخولك بواسطة العملة الظاهرية, ستطالب بـPIN المستخدم لإتمام المصادقة.

فئة الأجهزة كافة الأجهزة من نوع خاص، مثل محركات الأقراص.

قائمة جهات الاتصال الموثوق بها جدول خاص بجهات الاتصال الموثوق بها.

كشف عبارة عن مهمة تتيح للمستخدم إلغاء تشفير جلسة من سجل المحادثات أو أكثر من ذلك, عارضًا كنى جهات الاتصال بشكل نص عادي جعلاً الجلسة قابلة للعرض.

كلمة مرور الإلغاء عبارة عن كلمة مرور تنشأ عند طلب المستخدم شهادة جديدة. تتطلب كلمة المرور إذا رغب المستخدم في سحب شهادته/ها الرقمية. يضمن ذلك سحب الشهادة من قبل المستخدم فقط.

لوحة المعلومات مكان مركزي يمكنك من خلاله الوصول إلى ميزات وإعدادات هذا البرنامج' وإدارتها.

مجال عبارة عن مجموعة من الكمبيوترات والتي تعد جزءً من شبكة وتشارك قاعدة بيانات مشتركة للمكتبات. ولكل مجال اسم فريد, كما تخصص لكل مجال مجموعة مشتركة من القواعد والإجراءات.

مرسل آمن عبارة عن جهة اتصال موثوق بها ترسل الرسائل الإلكترونية ومستندات Microsoft Office الموقّعة و/أو المشفرة.

مسؤول راجع مسؤول Windows.

مسؤول Windows عبارة عن مستخدم يتمتع بالصلاحيات الكاملة لتعديل الأذونات وإدارة المستخدمين الآخرين.

مستخدم عبارة عن كافة المسجلين في Drive Encryption (تشفير محركات الأقراص). وتتاح للمستخدمين غير المسؤولين الصلاحيات المحددة فقط في Drive Encryption (تشفير محركات الأقراص). يتمكن هؤلاء من التسجيل (بعد موافقة المسؤول) وتسجيل الدخول فقط.

مستخدم مخول هو مستخدم تم منحه الإذن في عرض User Access Settings (إعدادات وصول المستخدم) لعرض إعدادات التكوين أو التعديل فيها في عروض Simple Configuration (التكوين البسيط) أو Device Class Configuration (تكوين فئات الأجهزة).

مصادقة عبارة عن إجراء التحقق من صلاحية المستخدم للقيام بمهمة ما مثل الوصول إلى الكمبيوتر, تعديل الإعدادات الخاصة ببرنامج معين, أو عرض المعلومات المحمية.

معلومات الاعتماد عبارة عن طريقة يثبت المستخدم من خلالها الأهلية للقيام بمهمة ما وذلك أثناء إجراء المصادقة.

مقياس حيوي عبارة عن فئة من اعتمادات المصادقة تستخدم الميزات البدنية, كبصمات الأصابع, للتعرف على المستخدم.

ملف تعريف التقطيع طريقة مسح محددة مع قائمة أصول.

موفر خدمة التشفير (CSP) عبارة عن موفر الخوارزميات أو مكتبتها والذيْن يمكن استخدامهما ضمن واجهة جيدة التعريف للقيام بوظائف تشفير معينة.

موقع مقترح عبارة عن مستخدم تم تعيينه من قبل صاحب مستند لـMicrosoft Word أو Microsoft Excel ليضيف سطر توقيع للمستند.

نظام ملفات التشفير (EFS) عبارة عن نظام يشفر كافة الملفات والمجلدات الفرعية في المجلد المحدد.

هوية في HP ProtectTools Security Manager (إدارة أمن HP ProtectTools)، مجموعة من بيانات الاعتماد والإعدادات التي يتم معالجتها كحساب أو ملف تعريف لمستخدم خاص.

وحدة تحكم مكان مركزي يمكنك من خلاله الوصول إلى ميزات وإعدادات هذا البرنامج' وإدارتها.

وضع جهاز SATA وضع لنقل البيانات بين الكمبيوتر وأجهزة تخزين كبيرة السعة, مثل محركات الأقراص الثابتة ومحركات الأقراص البصرية.

الفهرس