HP ProtectTools
מדריך למשתמש

© Copyright 2009 Hewlett-Packard Development Company, L.P.

Bluetooth הוא סימן מסחרי הנמצא בבעלות בעליו וחברת Hewlett-Packard משתמשת בו ברישיון. Java הוא סימן מסחרי בארה"ב של Sun Microsystems, Inc. ‏Microsoft ו-Windows הם סימנים מסחריים רשומים בארה"ב של Microsoft Corporation.

המידע הנכלל במסמך זה נתון לשינויים ללא הודעה מוקדמת. האחריות הבלעדית למוצרים ולשירותים של HP מפורטת במפורש בכתב האחריות הנלווה למוצרים ולשירותים אלו. אין להבין מתוך הכתוב לעיל כי תחול על המוצר אחריות נוספת כלשהי. חברת HP לא תישא באחריות לשגיאות טכניות או לשגיאות עריכה או להשמטות הכלולות במסמך זה.

מהדורה ראשונה: נובמבר 2009

מק"ט: 593308-BB1

תוכן העניינים

1 מבוא לאבטחה

מאפייני HP ProtectTools ... 2
השגת מטרות האבטחה העיקריות ... 3
הגנה מפני גניבה מתוכננת ... 3
הגבלת הגישה לנתונים רגישים ... 3
מניעה של גישה לא מורשית ממיקומים פנימיים או חיצוניים ... 3
יצירה של מדיניות סיסמאות חזקה ... 4
מרכיבי אבטחה נוספים ... 5
הקצאת תפקידי אבטחה ... 5
ניהול סיסמאות של HP ProtectTools ... 5
יצירת סיסמה מאובטחת ... 6
גיבוי ושחזור של הרשאות HP ProtectTools ... 6

2 תחילת העבודה עם אשף ההתקנה

3 HP ProtectTools Security Manager Administrative Console

פתיחת Administrative Console (מסוף הניהול) ... 10
שימוש ב-Administrative Console (מסוף הניהול) ... 11

4 הגדרת התצורה של המערכת

הגדרת אימות עבור המחשב ... 13
Logon Policy (מדיניות כניסה) ... 13
Session Policy (מדיניות הפעלה) ... 13
הגדרות ... 14
ניהול משתמשים ... 15
ציון הגדרות התקן ... 16
טביעות אצבע ... 16
כרטיס חכם ... 16
פנים ... 16
הגדרות מתקדמות ... 17

5 הגדרת התצורה של היישומים

הכרטיסייה General (כללי) ... 19

הכרטיסייה Applications (יישומים) 20

6 כלי ניהול
עדכונים והודעות 22

7 HP ProtectTools Security Manager
פתיחת HP ProtectTools Security Manager 24
שימוש בלוח המחוונים של Security Manager 25
הליכי הגדרה 26
רישום הרשאות 26
רישום טביעות אצבע 26
רישום סצינות 26
הגדרות מתקדמות למשתמש 27
שינוי סיסמת Windows 27
הגדרת כרטיס חכם 28
משימות כלליות 29
Password Manager (מנהל הסיסמאות) 29
עבור דפי אינטרנט או תוכניות שבהם לא נוצרו עדיין פרטי כניסה 29
עבור דפי אינטרנט או תוכניות שבהם כבר נוצרו פרטי כניסה 29
הוספת פרטי כניסה 30
עריכת פרטי כניסה 31
שימוש בתפריט Logons (פרטי כניסה) 31
סידור פרטי כניסה בקטגוריות 31
ניהול פרטי הכניסה 32
הערכת עוצמת הסיסמה 32
הגדרות סמל Password Manager (מנהל הסיסמאות) 32
הגדרות 33
הרשאות 33
כרטיס הזיהוי האישי שלך 34
הגדרת ההעדפות שלך 34
General (כללי) 34
Fingerprint (טביעת אצבע) 35
גיבוי ושחזור של הנתונים 35
Discover more (גלה עוד) 36
עדכונים והודעות 36
מצב יישומי אבטחה 36

8 Drive Encryption for HP ProtectTools (בדגמים נבחרים בלבד)
הליכי הגדרה 38
פתיחת Drive Encryption (הצפנת כונן) 38
משימות כלליות 39
הפעלת Drive Encryption (הצפנת כונן) 39
השבתת Drive Encryption (הצפנת כונן) 39

כניסה לאחר הפעלת Drive Encryption (הצפנת כונן) 39
הגנה על הנתונים על-ידי הצפנת הכונן הקשיח 40
הצגת מצב הצפנה 40
משימות מתקדמות 41
ניהול ה-Drive Encryption (הצפנת כונן) (משימה של מנהל מערכת) 41
הצפנה או פענוח של כוננים בודדים 41
גיבוי ושחזור (משימה של מנהל מערכת) 41
יצירת מפתחות גיבוי 41
ביצוע שחזור 42

9 Privacy Manager for HP ProtectTools (בדגמים נבחרים בלבד)

הליכי הגדרה 44
פתיחת Privacy Manager (מנהל הפרטיות) 44
ניהול אישורים של Privacy Manager (מנהל הפרטיות) 44
בקשה והתקנה של אישור Privacy Manager (מנהל הפרטיות) 44
בקשת אישור של Privacy Manager (מנהל הפרטיות) 45
השגת אישור חברה מוקצה מראש של Privacy Manager (מנהל הפרטיות) 45
התקנת האישור של Privacy Manager (מנהל הפרטיות) 45
הצגת פרטי האישור של Privacy Manager (מנהל הפרטיות) 46
חידוש אישור של Privacy Manager (מנהל הפרטיות) 46
הגדרת אישור ברירת מחדל של Privacy Manager (מנהל הפרטיות) 46
מחיקת אישור של Privacy Manager (מנהל הפרטיות) 46
שחזור אישור של Privacy Manager (מנהל הפרטיות) 47
ביטול אישור של Privacy Manager (מנהל הפרטיות) 47
ניהול אנשי קשר מהימנים 47
הוספת אנשי קשר מהימנים 48
הוספת איש קשר מהימן 48
הוספת אנשי קשר מהימנים באמצעות אנשי קשר של Microsoft Outlook 49
הצגת פרטי איש קשר מהימן 49
מחיקת איש קשר מהימן 49
בדיקת מצב הביטול של איש קשר מהימן 50
משימות כלליות 51
שימוש ב-Privacy Manager (מנהל הפרטיות) ב-Microsoft Outlook 51
הגדרת התצורה של Privacy Manager (מנהל הפרטיות) עבור Microsoft Outlook 51
חתימה ושליחה של הודעת דואר אלקטרוני 51
הוספת חותם ושליחה של הודעת דואר אלקטרוני 52
הצגת הודעת דואר אלקטרוני עם חותם 52
שימוש ב-Privacy Manager (מנהל הפרטיות) במסמך של Microsoft Office 2007 52
הגדרת התצורה של Privacy Manager (מנהל הפרטיות) עבור Microsoft Office 53
חתימה על מסמך Microsoft Office 53
הוספת שורת חתימה בעת חתימה על מסמך Microsoft Word או Microsoft Excel 53
הוספת חותמים מוצעים למסמך Microsoft Word או Microsoft Excel 53
הוספת שורת חתימה של חותם מוצע 54

הצפנת מסמך Microsoft Office 54
הסרת הצפנה ממסמך Microsoft Office 55
שליחת מסמך מוצפן של Microsoft Office 55
הצגת מסמך חתום של Microsoft Office 55
הצגת מסמך מוצפן של Microsoft Office 56
שימוש ב-Privacy Manager (מנהל הפרטיות) ב-Windows Live Messenger 56
התחלת הפעלת צ'אט של Privacy Manager (מנהל הפרטיות) 56
הגדרת התצורה של Privacy Manager (מנהל הפרטיות) עבור Windows Live Messenger 57
ניהול צ'אטים בחלון הצ'אט של Privacy Manager (מנהל הפרטיות) 57
הצגת היסטוריית צ'אטים 58
חשיפת כל ההפעלות 58
חשפית הפעלות של חשבון ספציפי 59
הצגת מזהה הפעלה 59
הצגת הפעלה 59
חיפוש טקסט ספציפי בהפעלות 59
מחיקת הפעלה 60
הוספה או הסרה של עמודות 60
סינון הפעלות מוצגות 60
משימות מתקדמות 62
העברת Privacy Manager Certificates (אישורים של מנהל הפרטיות) ו-Trusted Contacts (אנשי קשר מהימנים) למחשב אחר 62
גיבוי אישורים ואנשי קשר מהימנים של Privacy Manager (מנהל הפרטיות) 62
שחזור אישורים ואנשי קשר מהימנים של Privacy Manager (מנהל הפרטיות) 62
הניהול המרכזי של Privacy Manager (מנהל הפרטיות) 63

10 File Sanitizer for HP ProtectTools

גריסה 65
הלבנת שטח פנוי 66
הליכי הגדרה 67
פתיחת File Sanitizer (מנקה הקבצים) 67
הגדרת לוח זמנים לגריסה 67
הגדרת לוח זמנים להלבנת שטח פנוי 67
בחירה או יצירה של פרופיל גריסה 68
בחירת פרופיל גריסה מוגדר מראש 68
התאמה אישית של פרופיל גריסה 68
התאמה אישית של פרופיל מחיקה פשוטה 69
משימות כלליות 70
שימוש ברצף מקשים להפעלת גריסה 70
שימוש בסמל File Sanitizer (מנקה הקבצים) 71
גריסה ידנית של נכס אחד 71
גריסה ידנית של כל הפריטים שנבחרו 71
הפעלה ידנית של הלבנת שטח פנוי 72
ביטול פעולה של גריסה או הלבנת שטח פנוי 72

הצגת קובצי היומן 72

11 Device Access Manager for HP ProtectTools (בדגמים נבחרים בלבד)

הליכי הגדרה 74
פתיחת Device Access Manager (מנהל הגישה להתקנים) 74
הגדרת תצורה של גישה להתקנים 74
הקבוצה Device Administrators (מנהלי התקנים) 74
Simple Configuration (תצורה פשוטה) 74
הפעלת שירות ברקע 75
Device Class Configuration (תצורת מחלקות התקנים) 76
חסימת גישה של משתמש או קבוצה 77
מתן גישה למשתמש או קבוצה 77
הסרת גישה של משתמש או קבוצה 78
מתן גישה למחלקת התקנים עבור משתמש אחד מתוך קבוצה 78
הרשאת גישה להתקן ספציפי עבור משתמש אחד מתוך קבוצה 79
איפוס התצורה 79
משימות מתקדמות 80
בקרת גישה להגדרות התצורה 80
הענקת גישה לקבוצה או משתמש קיימים 80
חסימת גישה של קבוצה או משתמש קיימים 81
הוספת קבוצה או משתמש חדשים 81
הסרת גישה של קבוצה או משתמש 81
תיעוד קשור 81

12 LoJack Pro for HP ProtectTools

13 פתרון בעיות

HP ProtectTools Security Manager 83
Device Access Manager for HP ProtectTools 85
שונות 87

מילון מונחים 88

אינדקס 92

1 מבוא לאבטחה

תוכנת HP ProtectTools Security Manager מספקת מאפייני אבטחה המסייעים בהגנה כנגד גישה לא מורשית למחשב, לרשתות ולנתונים חיוניים. ניהול HP ProtectTools Security Manager מסופק באמצעות המאפיין Administrative Console (מסוף ניהול).

באמצעות המסוף HP ProtectTools Administrative Console, המנהל המקומי יכול לבצע את המשימות הבאות:

- הפעלה או השבתה של מאפייני האבטחה
- רישום טביעות האצבע שלהם ושל משתמשים אחרים במחשב זה
- רישום סצינה אחת או יותר לאימות הפנים
- הגדרת כרטיס חכם לאימות
- ציון הרשאות דרושות לאימות
- ניהול משתמשים במחשב
- כוונון פרמטרים ייחודיים להתקן
- קביעת התצורה של יישומי Security Manager (מנהל האבטחה) מותקנים
- הוספת יישומי Security Manager (מנהל האבטחה) נוספים

באמצעות לוח המחוונים של Security Manager, משתמשים כלליים יכולים לבצע את המשימות הבאות:

- הגדרת תצורה של אפשרויות שמסופקות על-ידי מנהל
- מתן אפשרות לבקרות מוגבלות של מספר מודולי HP ProtectTools

מודולי התוכנה הזמינים עבור המחשב שברשותך עשויים להשתנות בהתאם לדגם.

המודולים של תוכנת HP ProtectTools עשויים להיות מותקנים מראש, מוטענים מראש או זמינים להורדה מאתר האינטרנט של HP. לקבלת מידע נוסף, בקר בכתובת http://www.hp.com.

הערה: ההוראות במדריך זה מתייחסות לשלב שבו כבר התקנת את המודולים המתאימים של תוכנת HP ProtectTools.

מאפייני HP ProtectTools

הטבלה הבאה מפרטת את המאפיינים העיקריים של מודולי HP ProtectTools.

מודול	מאפייני מפתח
מסוף HP ProtectTools Security Manager Administrative Console (עבור מנהלים)	• הגדרה וקביעת תצורה של רמות אבטחה ושל שיטות כניסה מאובטחת באמצעות אשף ההתקנה של Security Manager. • קביעת תצורה של אפשרויות שמוסתרות ממשתמשים בסיסיים. • הגדרת תצורות Device Access Manager וגישת משתמש. • הוספה והסרה של משתמשי HP ProtectTools והצגת מצב המשתמש באמצעות כלי מנהל המערכת.
HP ProtectTools Security Manager (עבור משתמשים כלליים)	• ארגון, הגדרה ושינוי של שמות וסיסמאות משתמשים. • קביעת תצורה ושינוי של אישורי משתמש כגון סיסמת Windows ו-Smart Card (כרטיס חכם). • קביעת תצורה ושינוי של גריסה, הלבנה והגדרות של File Sanitizer. • הצגת הגדרות עבור Device Access Manager. • קביעת תצורה של העדפות ושל אפשרויות גיבוי ושחזור.
Credential Manager for HP ProtectTools (Password Manager)	• שמירה, ארגון והגנה על השמות והסיסמאות שלך. • הגדרת מסכי הכניסה של אתרי אינטרנט ותוכניות לקבלת גישה מהירה ומאובטחת. • שמירת שמות משתמשים וסיסמאות של אתרי אינטרנט באמצעות הזנתם לתוך Password Manager. בפעם הבאה שתבקר באתר זה, Password Manager ימלא וישלח את המידע באופן אוטומטי. • יצירת סיסמאות חזקות יותר עבור אבטחת חשבונות נוספת. Password Manager ממלא ושולח את המידע באופן אוטומטי.
Drive Encryption for HP ProtectTools (בדגמים נבחרים בלבד)	• אספקת הצפנה מלאה ומקיפה של הכונן הקשיח. • אילוץ של אימות לפני אתחול על מנת לפענח את הנתונים ולגשת אליהם.
Privacy Manager for HP ProtectTools (בדגמים נבחרים בלבד)	• שימוש בטכניקות כניסה מתקדמות כדי לאמת את המקור, התקינות והאבטחה של ההתקשרות באמצעות הדואר האלקטרוני, מסמכי Microsoft® Office או הודעות מיידית (IM).
File Sanitizer for HP ProtectTools	• גריסה של נכסים דיגיטליים (מידע רגיש, לרבות קובצי יישומים, תוכן היסטורי או תוכן הקשור לאינטרנט, או נתונים חסויים אחרים) במחשב שברשותך והלבנה מעת לעת של הכונן הקשיח.
Device Access Manager for HP ProtectTools (בדגמים נבחרים בלבד)	• מתן אפשרות למנהלי IT לשלוט על הגישה להתקנים בהתבסס על פרופילי משתמשים. • מניעה ממשתמשים לא מורשים לסלק נתונים באמצעות אמצעי אחסון חיצוני, ומניעה של הכנסת וירוסים למערכת מאמצעי חיצוני. • מתן אפשרות למנהלים להשבית גישה להתקנים ניתנים לכתיבה עבור אנשים מסוימים או קבוצות של משתמשים.

השגת מטרות האבטחה העיקריות

המודולים של HP ProtectTools יכולים לפעול יחד כדי לספק פתרונות עבור מגוון של בעיות אבטחה, לרבות מטרות האבטחה המרכזיות שלהלן:

- הגנה מפני גניבה מתוכננת
- הגבלת הגישה לנתונים רגישים
- מניעה של גישה לא מורשית ממיקומים פנימיים או חיצוניים
- יצירה של מדיניות סיסמאות חזקה

הגנה מפני גניבה מתוכננת

דוגמה של גניבה מתוכננת היא גניבה של מחשב המכיל מנתונים סודיים ופרטי הלקוחות בנקודת הבדיקות הביטחונית בשדה התעופה. המאפיינים הבאים מסייעים להגן מפני גניבה מתוכננת:

- מאפיין האימות במצב טרום-אתחול, אם מופעל, מסייע במניעת גישה למערכת ההפעלה. עיין בהליכים הבאים:
  - Security Manager (מנהל האבטחה)
  - Drive Encryption (הצפנת כונן)

הגבלת הגישה לנתונים רגישים

נניח שרואה חשבון חיצוני העובד באתר קבל גישה למחשב כדי לעיין בנתונים פיננסיים רגישים; אינך רוצה שרואה החשבון יוכל להדפיס את הקבצים או לשמור אותם להתקן הניתן לצריבה כגון תקליטור CD. המאפיין הבא מסייע להגביל את הגישה לנתונים:

- Device Access Manager for HP ProtectTools מאפשר למנהלי IT להגביל את הגישה להתקנים הניתנים לצריבה כך שלא תהיה אפשרות להדפיס או להעתיק את המידע הרגיש מהכונן הקשיח למדיה הניתנת להסרה.

מניעה של גישה לא מורשית ממיקומים פנימיים או חיצוניים

גישה לא מורשית למחשב עסקי לא מאובטח מהווה סיכון ממשי ביותר למשאבי רשת ארגוניים, כגון מידע משירותים פיננסיים, מנהל בכיר או צוות מחקר ופיתוח, ולמידע אישי כגון תיעוד של מטופלים או תיעוד פיננסי אישי. המאפיינים הבאים מסייעים במניעת גישה לא מורשית:

- מאפיין האימות במצב טרום-אתחול, אם מופעל, מסייע במניעת גישה למערכת ההפעלה. עיין בהליכים הבאים:
  - Password Manager (מנהל הסיסמאות)
  - Drive Encryption (הצפנת כונן)
- Password Manager (מנהל הסיסמאות) מסייע להבטיח שמשתמש לא מורשה לא יקבל סיסמאות או גישה ליישומים המוגנים באמצעות סיסמה.
- Device Access Manager for HP ProtectTools מאפשר למנהלי IT להגביל את הגישה להתקנים הניתנים לצריבה כך שלא תהיה אפשרות להעתיק את המידע הרגיש מהכונן הקשיח.
- File Sanitizer מאפשר מחיקה בטוחה של נתונים באמצעות גריסה של תיקיות וקבצים קריטיים או הלבנת הכונן הקשיח (כתיבה על נתונים שנמחקו אך עדיין ניתנים לשחזור).
- DriveLock מסייע להבטיח שלא תהיה אפשרות לגשת לנתונים אפילו אם הכונן הקשיח יוסר ויותקן במערכת לא מאובטחת.

יצירה של מדיניות סיסמאות חזקה

אם הרשאה נכנסת לתוקף הדורש את השימוש במדיניות סיסמאות חזקה עבור עשרות יישומים ומסדי הנתונים מבוססי האינטרנט, Security Manager (מנהל האבטחה) מספק מאגר סיסמאות מוגן ונוחיות של Single Sign On (כניסה יחידה).

מרכיבי אבטחה נוספים

הקצאת תפקידי אבטחה

במסגרת הניהול של אבטחת מחשבים (בייחוד עבור ארגונים גדולים), נוהל אחד חשוב הוא חלוקה של תחומי האחריות והזכויות בין סוגים שונים של מנהלי מערכת ומשתמשים.

הערה: בארגון קטן או לצורך שימוש אישי, תפקידים אלה יכולים להתבצע על-ידי אותו אדם.

עבור HP ProtectTools, ניתן לחלק את החובות והזכויות הכרוכות באבטחה לתפקידים הבאים:

- מנהל האבטחה - מגדיר את רמת האבטחה עבור החברה או הרשת וקובע את מאפייני האבטחה שאותם יש לפרוס, כגון כרטיסי Java™ Card, קוראים ביומטריים או Token של USB.

הערה: רבים מהמאפיינים ב-HP ProtectTools ניתנים להתאמה אישית על-ידי מנהל האבטחה בשיתוף עם HP. לקבלת מידע נוסף, בקר באתר האינטרנט של HP בכתובת http://www.hp.com.

- מנהל—מחיל ומנהל את מאפייני האבטחה המוגדרים על-ידי קצין הביטחון. יכול גם להפעיל ולהשבית מספר מאפיינים. לדוגמה, אם קצין הביטחון החליט לפרוס כרטיסי Java Cards, מנהל ה-IT יכול להפעיל את מצב האבטחה Java Card BIOS.
- משתמש - עושה שימוש במאפייני האבטחה. לדוגמה, אם מנהל האבטחה ומנהל ה-IT הפעילו כרטיסי Java Card עבור המערכת, המשתמש יכול להגדיר מספר זיהוי אישי (PIN) של כרטיס Java Card ולהשתמש בכרטיס לצורך אימות.

זהירות: המנהלים מוזמנים להשתמש בשיטות העבודה המומלצות בהגבלת הרשאות של משתמשי קצה ובהגבלת גישת משתמשים.

אין להעניק למשתמשים לא מורשים הרשאות של מנהל המערכת.

ניהול סיסמאות של HP ProtectTools

רוב המאפיינים של HP ProtectTools Security Manager מאובטחים באמצעות סיסמאות. הטבלה הבאה מפרטת את הסיסמאות הנמצאות בשימוש נפוץ, מודול התוכנה שבו הסיסמה מוגדרת ופונקציית הסיסמה.

הסיסמאות שאותן מגדירים ושבהן משתמשים מנהלי ה-IT מפורטות גם הן בטבלה זו. כל שאר הסיסמאות מוגדרות על-ידי משתמשים או מנהלי מערכת רגילים.

סיסמת HP ProtectTools	הגדרה במודול שלהלן	פונקציה
סיסמת כניסה של Windows	לוח הבקרה של ®Windows או HP ProtectTools Security Manager	ניתן להשתמש לכניסה ידנית ולאימות לצורך גישה למאפיינים שונים של Security Manager (מנהל האבטחה).
סיסמת הגיבוי והשחזור של Security Manager (מנהל האבטחה)	Security Manager (מנהל האבטחה), על-ידי משתמש נפרד	להגנה על הגישה לקובץ הגיבוי והשחזור של Security Manager (מנהל האבטחה).
PIN של כרטיסי Java™ Card	Java Card Security (אבטחת כרטיסי Java)	מגן על הגישה לתוכן של כרטיס Java Card ומאמת משתמשים של כרטיס Java Card. כאשר הוא משמש לאימות במהלך הפעלה, ה-PIN של כרטיס ה-Java Card גם מגן על הגישה לתוכנית השירות Computer Setup (הגדרות המחשב) ולתוכן המחשב. מאמת משתמשים של Drive Encryption (הצפנת כונן), אם נבחר Token של כרטיס Java Card.

יצירת סיסמה מאובטחת

בעת יצירת סיסמאות, תחילה עליך לפעול בהתאם למפרטים המוגדרים על-ידי התוכנית. עם זאת, באופן כללי עליך לשקול את ההנחיות הבאות שיסייעו לך ליצור סיסמאות חזקות ויפחיתו את הסיכוי לכך שהסיסמה שלך תיחשף:

- השתמש בסיסמאות הכוללות למעלה מ-6 תווים, מומלץ למעלה מ-8.
- שלב בסיסמה שלך אותיות רישיות וקטנות.
- במידת האפשר, השתמש בשילוב של תווים אלפא-נומריים והוסף תווים מיוחדים וסימני פיסוק.
- השתמש בתווים מיוחדים או במספרים במקום אותיות במילת מפתח. לדוגמה, באפשרותך להשתמש במספר 1 לייצוג האותיות I או L.
- שלב מילים משתי שפות או יותר.
- פצל מילה או ביטוי על-ידי הוספת מספרים או תווים מיוחדים באמצע, לדוגמה, "Mary2-2Cat45".
- אל תשתמש בסיסמה שתופיע במילון.
- אל תשתמש בשם שלך כסיסמה, או בכל פרט אישי אחר, כגון תאריך לידה, שמות של חיות מחמד או שם הנעורים של האם, גם אם אתה מאיית אותו מהסוף להתחלה.
- החלף סיסמאות באופן קבוע. ייתכן שתשנה רק שני תווים שיתווספו.
- אם אתה רושם את הסיסמה שלך, אל תשמור אותה במקום נראה לעין בקרבת המחשב.
- אל תשמור סיסמאות בקובץ, כגון הודעת דואר אלקטרוני, במחשב.
- אל תשתף חשבונות ואל תמסור לאף אחד את הסיסמה שלך.

גיבוי ושחזור של הרשאות HP ProtectTools

באפשרותך להשתמש במאפיין הגיבוי והשחזור של HP ProtectTools לבחירה ולגיבוי של נתוני אישורים והגדרות של HP ProtectTools.

2 תחילת העבודה עם אשף ההתקנה

אשף ההתקנה של HP ProtectTools מדריך אותך לאורך ההגדרה של המאפיינים הנפוצים ביותר של Security Manager. עם זאת, ישנה פונקציונליות נוספת ורבה הזמינה באמצעות HP ProtectTools Administrative Console. ניתן להגדיר את התצורה של אותן ההגדרות שנמצאות באשף, כמו גם מאפייני אבטחה נוספים, באמצעות המסוף שאליו ניתן לגשת מתפריט Start (התחלה) של ®Windows. הגדרות אלה חלות על המחשב ועל כל המשתמשים המשתפים את המחשב.

1. שבוע לאחר ההגדרה הראשונית של המחשב, בעת כניסתך למערכת או כאשר משתמש בעל הרשאות מנהל מעביר אצבע בקורא טביעות האצבע בפעם הראשונה, אשף ההתקנה של Security Manager יתחיל להדריך אותך באופן אוטומטי בשלבים הבסיסיים של הגדרת התצורה של התוכנית. ערכת לימוד בווידאו בנושא הגדרת המחשב תופעל באופן אוטומטי.

   - לחלופין -

   פתח את HP ProtectTools Security Manager מסמל ה**גאדג'ט** בסרגל הצידי של Windows או מסמל שורת המשימות באזור ההודעות, בקצה הימני של שורת המשימות.

   הצבע של הסרגל העליון בסמל הגאדג'ט מציין אחד מהמצבים הבאים:

   - אדום—HP ProtectTools לא הוגדר, או שקיים מצב שגיאה באחד ממודולי ה-ProtectTools.
   - צהוב—סמן את הדף Applications Status (מצב יישומים) ב-Security Manager עבור שינויי הגדרות שיש לבצע.
   - כחול—HP ProtectTools הוגדר, והוא פועל כהלכה.

   הערה: סמל הגאדג'ט אינו זמין ב-Windows XP.

   - לחלופין -

   לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), ולאחר מכן לחץ על **HP ProtectTools Administrative Console**.

2. קרא את מסך הפתיחה ולאחר מכן לחץ על **Next** (הבא).

   הערה: במסך הפתיחה, באפשרותך להשבית כל הצגה נוספת של האשף על-ידי בחירת אחת מהאפשרויות.

3. אשף ההתקנה יבקש ממך לאמת את זהותך.

הקלד את סיסמת Windows שלך או סרוק את טביעות האצבע שלך באמצעות קורא טביעות האצבע, ולאחר מכן לחץ על **Next** (הבא).

אם קורא טביעות אצבע או כרטיס חכם אינם זמינים, תתבקש להזין את סיסמת Windows. יש להשתמש בסיסמה זו בעתיד בכל פעם שנדרש אימות.

אם טרם יצרת סיסמת Windows, אתה מתבקש לעשות זאת. סיסמת Windows נדרשת להגנה על חשבון Windows מפני גישה של אנשים בלתי מורשים ולשימוש במאפיינים של HP ProtectTools Security Manager.

4. אשף ההתקנה ידריך אותך לאורך התהליך של הגדרת מאפייני האבטחה שחלים על כל המשתמשים במחשב:

- המאפיין Windows Logon Security (אבטחת הכניסה של Windows) מגן על חשבונות Windows על-ידי דרישת שימוש בהרשאות מסוימות לצורך גישה.
- המאפיין Drive Encryption (הצפנת כונן) מגן על הנתונים על-ידי הצפנת הכוננים הקשיחים והפיכת המידע לבלתי קריא לאנשים ללא ההרשאה המתאימה.
- המאפיין Pre-Boot Security (אבטחת טרום-אתחול) מגן על המחשב על-ידי איסור גישה של אנשים בלתי מורשים לפני אתחול Windows.

הערה: Pre-Boot Security (אבטחת טרום-אתחול) אינו זמין אם ה-BIOS של המחשב לא תומך בכך.

כדי להפעיל מאפיין אבטחה, בחר בתיבת הסימון שלו. ככל שתבחר מאפיינים רבים יותר, כך המחשב יהיה מאובטח יותר.

5. בדף האחרון של האשף, לחץ על **Finish** (סיום).

לוח המחוונים של Security Manager מוצג.

הערה: אם לא תשלים את האשף, הוא יופעל באופן אוטומטי עוד פעמיים. לאחר מכן, תוכל לגשת לאשף מבלון ההודעות שמופיע באזור ההודעות בקצה הימני או השמאלי של שורת המשימות (אלא אם השבתת אותו) עד להשלמת ההגדרה.

3 HP ProtectTools Security Manager Administrative Console

ניהול HP ProtectTools Security Manager מסופק באמצעות Administrative Console (מסוף ניהול).

הערה: ניהול HP ProtectTools דורש הרשאות של מנהל מערכת.

המסוף מספק את המאפיינים הבאים:

- הפעלה או השבתה של מאפייני האבטחה
- ניהול משתמשים במחשב
- כוונון פרמטרים ייחודיים להתקן
- קביעת תצורה של יישומי Security Manager
- הוספת יישומי Security Manager נוספים

▲ כדי להשתמש ביישומי HP ProtectTools Security Manager, הפעל את HP ProtectTools Security Manager מתפריט Start (התחלה) או לחץ לחיצה ימנית על סמל Security Manager באזור ההודעות, הממוקם בקצה הימני או השמאלי של שורת המשימות.

HP ProtectTools Administrative Console והיישומים שלו זמינים לכל המשתמשים המשתפים את המחשב.

פתיחת Administrative Console (מסוף הניהול)

עבור משימות ניהול, כגון הגדרת מדיניות מערכת או הגדרת תצורה של תוכנה, פתח את המסוף באופן הבא:

▲ לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), לחץ על **HP** ולאחר מכן לחץ על **HP ProtectTools Administrative Console**.

- לחלופין -

בלוח השמאלי או הימני בלוח המחוונים של Security Manager, לחץ על **Administration** (ניהול).

עבור משימות משתמש, כגון רישום טביעות אצבע או שימוש ב-Security Manager, פתח את המסוף באופן הבא:

▲ לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), לחץ על **HP** ולאחר מכן לחץ על **HP ProtectTools Security Manager**.

- לחלופין -

לחץ לחיצה כפולה על סמל **HP ProtectTools Security Manager** באזור ההודעות, בקצה הימני או השמאלי של שורת המשימות.

שימוש ב-Administrative Console (מסוף הניהול)

מסוף Security Manager Administrative Console הוא המיקום המרכזי עבור ניהול של HP ProtectTools Security Manager.

המסוף מורכב מהרכיבים הבאים:

- **Tools** (כלים)—הרכיב מציג את הקטגוריות הבאות להגדרת התצורה של האבטחה במחשב:
  - **Home** (בית)—הרכיב מאפשר לך לבחור את משימות האבטחה לביצוע.
  - **System** (מערכת)—הרכיב מאפשר לך להגדיר תצורה של מאפייני אבטחה ואימות עבור משתמשים והתקנים.
  - **Applications** (יישומים)—הרכיב מציג הגדרות כלליות עבור HP ProtectTools Security Manager ויישומי Security Manager.
  - **Data** (נתונים)—הרכיב מספק תפריט מתרחב של קישורים ליישומי Security Manager המגנים על הנתונים.
- **Management Tools** (כלי ניהול)—מספק מידע על כלים נוספים. הלוח מציג את האפשרויות הבאות:
  - **HP ProtectTools Security Manager Setup Wizard** (אשף ההתקנה של HP ProtectTools Security Manager)—האשף מדריך אותך לאורך ההגדרה של HP ProtectTools Security Manager.
  - **Help** (עזרה)—מציג את קובץ העזרה, אשר מספק מידע אודות Security Manager והיישומים שלו המותקנים מראש. עזרה עבור יישומים שאתה מוסיף מופיעה בתוך יישומים אלה.
  - **About** (אודות)—מציג מידע אודות HP ProtectTools Security Manager, כגון מספר הגרסה והודעת זכויות יוצרים.
- **Main area** (האזור הראשי)—הרכיב מציג מסכים הספציפיים ליישומים.

4 הגדרת התצורה של המערכת

ניתן לגשת לקבוצה System (מערכת) מלוח תפריט Tools (כלים) בצד השמאלי או הימני של מסך HP ProtectTools Administrative Console. באפשרותך להשתמש ביישומים בקבוצה זו כדי לנהל את המדיניות וההגדרות של המחשב, המשתמשים וההתקנים שלו.

היישומים הבאים כלולים בקבוצה System (מערכת):

- **Security** (אבטחה)—נהל מאפיינים, אימות והגדרות הקובעות כיצד משתמשים יתקשרו עם מחשב זה.
- **Users** (משתמשים)—הגדר, נהל ורשום משתמשים של מחשב זה.
- **Devices** (התקנים)—נהל הגדרות של התקני אבטחה המובנים במחשב או מחוברים אליו.

הגדרת אימות עבור המחשב

בתוך היישום Authentication (אימות), באפשרותך לבחור את מאפייני האבטחה שתיישם במחשב, להגדיר מדיניות השולטת בגישה למחשב ולהגדיר תצורה של הגדרות מתקדמות נוספות. באפשרותך לציין את ההרשאות הדרושות לאימות כל מחלקת משתמשים בעת הכניסה ל-Windows או לאתרי אינטרנט ותוכניות במהלך הפעלת המשתמש.

כדי להגדיר אימות במחשב:

1. בתפריט הלוח Security (אבטחה), לחץ על **Authentication** (אימות).
2. כדי להגדיר תצורה של אימות כניסה, לחץ על הכרטיסייה **Logon Policy** (מדיניות כניסה), בצע שינויים ולחץ על **Apply** (החל).
3. כדי להגדיר תצורה של אימות הפעלה, לחץ על הכרטיסייה **Session Policy** (מדיניות הפעלה), בצע שינויים ולחץ על **Apply** (החל).

Logon Policy (מדיניות כניסה)

כדי להגדיר מדיניות השולטת בהרשאות הדרושות לאימות משתמשים בעת הכניסה ל-Windows:

1. בתפריט Tools (כלים), לחץ על **Security** (אבטחה) ולאחר מכן לחץ על **Authentication** (אימות).
2. בכרטיסייה **Logon Policy** (מדיניות כניסה), לחץ על קטגוריית משתמשים.
3. ציין את הרשאות האימות הדרושות עבור קטגוריית המשתמשים שנבחרה. יש לציין הרשאה אחת לפחות.
4. בחר אם כל אחת מההרשאות שצוינו (הרשאה אחת) או אם כל ההרשאות שצוינו דרושות לאימות המשתמש. כמו כן, באפשרותך למנוע גישה למחשב של משתמשים כלשהם.
5. לחץ על **Apply** (החל).

Session Policy (מדיניות הפעלה)

כדי להגדיר מדיניות השולטת בהרשאות הדרושות לגישה ליישומי HP ProtectTools במהלך הפעלת Windows:

1. בתפריט Tools (כלים), לחץ על **Security** (אבטחה) ולאחר מכן לחץ על **Authentication** (אימות).
2. בכרטיסייה **Session Policy** (מדיניות הפעלה), לחץ על קטגוריית משתמשים.
3. ציין את הרשאות האימות הדרושות עבור קטגוריית המשתמשים שנבחרה.
4. בחר אם לאימות משתמש דרושה הרשאה אחת שצוינה או כל ההרשאות שצוינו. כמו כן, באפשרותך שלא לדרוש אימות לגישה לתוכנת HP ProtectTools.
5. לחץ על **Apply** (החל).

הגדרות

באפשרותך לאפשר הגדרה אחת או יותר מבין הגדרות האבטחה הבאות:

- **Allow One Step logon** (מתן אפשרות לכניסה יחידה)—ההגדרה מאפשרת למשתמשי המחשב לדלג על הכניסה ל-Windows אם האימות בוצע ברמת ה-BIOS או הדיסק המוצפן.
- **Allow HP SpareKey authentication for Windows logon** (מתן אפשרות לאימות HP SpareKey עבור הכניסה ל-Windows)—ההגדרה מאפשרת למשתמשי המחשב להשתמש במאפיין HP SpareKey לכניסה ל-Windows, למרות מדיניות אימות אחרת כלשהי שדורש Security Manager (מנהל האבטחה).

כדי לערוך את ההגדרות:

1. לחץ כדי להפעיל או להשבית הגדרה ספציפית.
2. לחץ על **Apply** (החל) כדי לשמור את השינויים שביצעת.

ניהול משתמשים

בתוך היישום Users (משתמשים), באפשרותך לנטר ולנהל את משתמשי HP ProtectTools של מחשב זה.

כל משתמשי HP ProtectTools רשומים ומאומתים מול המדיניות שהוגדרה באמצעות Security Manager (מנהל האבטחה), גם אם לא רשמו את ההרשאות המתאימות המאפשרות להם לעמוד במדיניות זו.

לניהול משתמשים, בחר מתוך ההגדרות הבאות:

- כדי להוסיף משתמשים, לחץ על **Add** (הוסף).
- כדי למחוק משתמש, לחץ על המשתמש ולאחר מכן לחץ על **Delete** (מחק).
- כדי לרשום טביעות אצבע או להגדיר הרשאות נוספות עבור המשתמש, לחץ על המשתמש ולאחר מכן לחץ על **Enroll** (רשום).
- כדי להציג את המדיניות של משתמש ספציפי, בחר את המשתמש והצג את המדיניות בחלון התחתון.

ציון הגדרות התקן

בתוך היישום Device (התקן), באפשרותך לציין הגדרות הזמינות עבור כל התקן אבטחה מובנה או מחובר ש-HP ProtectTools Security Manager מזהה.

טביעות אצבע

הדף Fingerprints (טביעות אצבע) מכיל שלוש כרטיסיות: Enrollment (רישום), Sensitivity (רגישות) ו-Advanced (מתקדם).

Enrollment (רישום)

באפשרותך לבחור את מספר טביעות האצבע המינימלי והמקסימלי שמשתמשים רשאים לרשום.

כמו כן, באפשרותך לנקות את כל הנתונים מקורא טביעות האצבע.

△ **זהירות:** ניקוי כל הנתונים מקורא טביעות האצבע מוחק את כל נתוני טביעות האצבע של כל המשתמשים, לרבות מנהלי מערכות. אם מדיניות הכניסה דורשת טביעות אצבע בלבד, ניתן למנוע מכל המשתמשים להיכנס למחשב.

Sensitivity (רגישות)

כדי לכוונן את הרגישות של קורא טביעות האצבע בעת סריקת טביעות האצבע, הזז את המחוון.

אם טביעת האצבע שלך אינה מזוהה באופן עקבי, ייתכן שיש צורך בהגדרת רגישות נמוכה יותר. הגדרה גבוהה יותר מגבירה את הרגישות לשינויים בסריקות של טביעות אצבע ולפיכך מפחיתה את האפשרות של אישור שגוי. ההגדרה הבינונית-גבוהה מספקת שילוב טוב של אבטחה ונוחות.

Advanced (מתקדם)

באפשרותך להגדיר את התצורה של קורא טביעות האצבע כדי לחסוך במתח כאשר המחשב פועל באמצעות סוללה.

כרטיס חכם

באפשרותך להגדיר את תצורת המחשב להינעל באופן אוטומטי בעת הסרת כרטיס חכם. עם זאת, המחשב יינעל רק אם הכרטיס החכם שימש כהרשאת אימות בעת הכניסה ל-Windows. הסרת כרטיס חכם שלא שימש לכניסה ל-Windows לא תנעל את המחשב.

▲ בחר את תיבת הסימון כדי להפעיל או להשבית את נעילת המחשב בעת הסרת הכרטיס החכם.

פנים

באפשרותך להגדיר את רמת האבטחה לצורך זיהוי הפנים כדי לאזן בין קלות השימוש לקושי שבהפרת האבטחה של המחשב.

1. לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), לחץ על **HP** ולאחר מכן לחץ על **HP ProtectTools Administrative Console**.
2. לחץ על **Devices** (התקנים) ולאחר מכן לחץ על **Face** (פנים).

3. לנוחות רבה אף יותר, לחץ על המחוון כדי להסיטו שמאלה, או לקבלת דיוק רב יותר, לחץ על המחוון כדי להסיטו ימינה.

- **Convenience** (נוחות)—כדי להקל על קבלת הגישה של המשתמשים הרשומים בעת מצבים גבוליים, לחץ על המחוון כדי להסיטו למיקום **Convenience** (נוחות).
- **Balance** (איזון)—כדי להגיע לפשרה נוחה בין אבטחה לשימושיות, או אם ברשותך מידע רגיש או אם המחשב שברשותך ממוקם באזור שבו בוצעו ניסיונות כניסה לא מורשית, לחץ על המחוון כדי להסיטו למיקום **Balance** (איזון).
- **Accuracy** (דיוק)—כדי להקשות על משתמש לקבל גישה אם הסצינות הרשומות או תנאי התאורה הקיימים אינם רגילים וכדי להפחית את האפשרות של אישור שגוי, לחץ על המחוון כדי להסיטו למיקום **Accuracy** (דיוק).

הערה: רמת האבטחה חלה על כל המשתמשים

4. לחץ על **Apply** (החל).

הגדרות מתקדמות

1. לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), לחץ על **HP** ולאחר מכן לחץ על **HP ProtectTools Administrative Console**.
2. לחץ על **Devices** (התקנים) ולאחר מכן לחץ על **Face** (פנים).
3. לחץ על **Advanced** (מתקדם).
   - **לא לדרוש שם משתמש לצורך כניסה ל-Windows.**
     - בחר בתיבת הסימון כדי לאפשר למשתמשים להיכנס ל-Windows ללא שם משתמש.
     - נקה את תיבת הסימון כדי לדרוש שם משתמש לצורך כניסה.
   - **דרישה להשתמש ב-PIN לכניסה באמצעות זיהוי הפנים**—בחר בתיבת הסימון כדי לדרוש מכל משתמש להגדיר את PIN (מספר זיהוי אישי) ולהשתמש בו לצורך כניסה.
     - **האורך המינימלי המורשה עבור PIN**—לחץ על החץ למעלה כדי להגדיל או על החץ למטה כדי להקטין את מספר התווים המינימלי הנדרש עבור PIN.
     - **האורך המקסימלי המורשה עבור PIN**—לחץ על החץ למעלה כדי להגדיל או על החץ למטה כדי להקטין את מספר התווים המקסימלי המורשה עבור PIN.
     - **המספר המקסימלי המורשה של ניסיונות חוזרים עבור PIN**—לחץ על החץ למעלה כדי להגדיל או על החץ למטה כדי להקטין את מספר הפעמים המקסימלי של הזנות PIN חוזרות.
4. לחץ על **OK** (אישור).

5 הגדרת התצורה של היישומים

ניתן לגשת לקבוצה Applications (יישומים) מתפריט הלוח Security Applications (יישומי אבטחה) בצד השמאלי או הימני של HP ProtectTools Administrative Console. באפשרותך להשתמש ב-Settings (הגדרות) כדי להתאים אישית את אופן הפעולה של היישומים המותקנים של HP ProtectTools Security Manager.

כדי לערוך את הגדרות היישומים:

1. בתפריט Tools (כלים), מתוך הקבוצה **Applications** (יישומים), לחץ על **Settings** (הגדרות).
2. לחץ כדי להפעיל או להשבית הגדרה ספציפית.
3. לחץ על **Apply** (החל) כדי לשמור את השינויים שביצעת.

הכרטיסייה General (כללי)

ההגדרות הבאות זמינות בכרטיסייה General (כללי):

- **Do not automatically launch the Setup Wizard for administrators** (אל תפעיל את אשף ההתקנה באופן אוטומטי עבור מנהלי מערכת)—בחר אפשרות זו כדי למנוע פתיחה אוטומטית של האשף בכניסה.
- **Do not automatically launch the Getting Started wizard for users** (אל תפעיל את אשף תחילת העבודה באופן אוטומטי עבור משתמשים)—בחר אפשרות זו כדי למנוע פתיחה אוטומטית של הגדרת המשתמש בכניסה.

הכרטיסייה Applications (יישומים)

ההגדרות המוצגות כאן יכולות להשתנות עם הוספת יישומים חדשים ל-Security Manager (מנהל האבטחה). הגדרות המינימום המוצגות כברירת מחדל הן:

- **Applications status** (מצב יישומים)—ההגדרה מפעילה את הצגת המצב עבור כל היישומים.
- **Password Manager** (מנהל הסיסמאות)—ההגדרה מפעילה את היישום Password Manager (מנהל הסיסמאות) עבור כל משתמשי המחשב.
- **Privacy Manager** (מנהל הפרטיות)—ההגדרה מפעילה את היישום Privacy Manager (מנהל הפרטיות) עבור כל משתמשי המחשב.
- **Enable the Discover more button** (הפעל את הלחצן 'גלה עוד')—ההגדרה מאפשרת לכל משתמשי המחשב להוסיף יישומים ל-HP ProtectTools Security Manager על-ידי לחיצה על הלחצן **[+] Discover more** (גלה עוד).

כדי להחזיר את כל היישומים להגדרות היצרן, לחץ על הלחצן **Restore Defaults** (שחזר ברירות מחדל).

6 כלי ניהול

ייתכן שיישומים נוספים יהיו זמינים להוספת כלי ניהול חדשים ל-Security Manager. מנהל המערכת של מחשב זה יכול להשבית מאפיין זה באמצעות היישום Settings (הגדרות).

כדי להוסיף כלי ניהול נוספים, לחץ על **Management tools [+]** (כלי ניהול).

עדכונים והודעות

אם חיבור לאינטרנט זמין, באפשרותך לגשת לאתר האינטרנט של DigitalPersona בכתובת http://www.digitalpersona.com/ כדי לחפש אחר יישומים חדשים או כדי להגדיר לוח זמנים לעדכונים אוטומטיים.

1. כדי לבקש מידע לגבי יישומים ועדכונים חדשים, בחר בתיבת הסימון **ברצוני לקבל הודעות לגבי יישומים ועדכונים חדשים.**
2. כדי להגדיר תזמון עבור עדכונים אוטומטיים, בחר את מספר הימים.
3. כדי לחפש עדכונים, לחץ על **Check Now** (בדוק כעת).

7 HP ProtectTools Security Manager

HP ProtectTools Security Manager מאפשר לך לשפר במידה רבה את אבטחת המחשב.

באפשרותך להשתמש ביישומי Security Manager (מנהל האבטחה) הטעונים מראש, כמו גם ביישומים נוספים הזמינים להורדה מיידית מהאינטרנט:

- נהל כניסות וסיסמאות
- שנה בקלות את סיסמת מערכת ההפעלה ®Windows
- הגדר העדפות תוכנית
- השתמש בטביעות אצבע לשיפור האבטחה והנוחות
- רשום סצינה אחת או יותר לאימות
- הגדר כרטיס חכם לאימות
- גבה ושחזר את נתוני התוכניות
- הוסף יישומים נוספים

פתיחת HP ProtectTools Security Manager

באפשרותך לפתוח את HP ProtectTools Security Manager בכל אחת מהדרכים הבאות:

- לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), לחץ על **HP** ולאחר מכן לחץ על **HP ProtectTools Security Manager**.
- לחץ לחיצה כפולה על סמל **HP ProtectTools** באזור ההודעות, בקצה הימני או השמאלי של שורת המשימות.
- לחץ לחיצה ימנית על סמל **HP ProtectTools** ולחץ על **Open HP ProtectTools Security Manager** (פתח את HP ProtectTools Security Manager).
- לחץ על האביזר **Security Manager ID Card** (כרטיס זיהוי של מנהל האבטחה) בסרגל הצידי של Windows.
- הקש את שילוב המקש החם ctrl+Windows+h כדי לפתוח את תפריט Quick Links (קישורים מהירים) של Security Manager.

שימוש בלוח המחוונים של Security Manager

לוח המחוונים של Security Manager הוא המיקום המרכזי שממנו ניתן לגשת בקלות למאפיינים, ליישומים ולהגדרות של Security Manager.

▲ כדי לפתוח את לוח המחוונים של Security Manager, לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), לחץ על **HP** ולאחר מכן לחץ על **HP ProtectTools Security Manager**.

לוח המחוונים מורכב מהרכיבים הבאים:

- **ID Card** (כרטיס זיהוי)—הרכיב מציג את שם המשתמש של Windows ותמונה נבחרת המזהה את חשבון המשתמש שנכנס.
- **Security Applications** (יישומי אבטחה)—הרכיב מציג תפריט מתרחב של קישורים להגדרת תצורה של קטגוריות האבטחה הבאות:
  - **Credential Manager**
  - **My Data (הנתונים שלי)**
- **Discover more** (גלה עוד)—הרכיב פותח דף שבו ניתן למצוא יישומים נוספים לשיפור האבטחה של הזהות, הנתונים והתקשורת.
- **Main area** (האזור הראשי)—הרכיב מציג מסכים הספציפיים ליישומים.
- **Administration** (ניהול)—הרכיב פותח את HP ProtectTools Administrative Console.
- **לחצן Help** (עזרה)—הרכיב מציג מידע אודות המסך הנוכחי.
- **Advanced** (מתקדם)—הרכיב מאפשר לך לגשת לאפשרויות הבאות:
  - **Preferences** (העדפות)—האפשרות מאפשרת לך להתאים אישית את ההגדרות של Security Manager.
  - **Backup and Restore** (גיבוי ושחזור)—האפשרות מאפשרת לך לגבות או לשחזר נתונים.
  - **About** (אודות)—האפשרות מציגה מידע גרסה של Security Manager.

הליכי הגדרה

רישום הרשאות

באפשרותך להשתמש בדף My Identity (הזהות שלי) כדי לרשום את שיטות האימות השונות או ההרשאות. לאחר הרישום, תוכל להשתמש בשיטות אלה לכניסה ל-Security Manager.

רישום טביעות אצבע

אם המחשב כולל קורא טביעות אצבע מובנה או מחובר, אשף ההתקנה של HP ProtectTools Security Manager ידריך אותך לאורך התהליך של ההגדרה או "הרישום" של טביעות האצבעות.

1. מוצג מתאר של שתי כפות ידיים. אצבעות שכבר נרשמו מודגשות בירוק. לחץ על אצבע במתאר.

> **הערה:** כדי למחוק טביעת אצבע שנרשמה קודם, לחץ על האצבע שלה.

2. לאחר שבחרת אצבע לרישום, תתבקש לסרוק את האצבע עד לרישומה המוצלח של טביעת האצבע. אצבע שנרשמה מודגשת בירוק במתאר.

3. יש לרשום שתי אצבעות לפחות; האצבע המורה או האמה הן המועדפות. חזור על שלבים 1 עד 3 עבור אצבע אחרת.

4. לחץ על **Next** (הבא) ולאחר מכן עקוב אחר ההוראות שעל-גבי המסך.

> **הערה:** בעת רישום טביעות אצבע באמצעות תהליך תחילת העבודה, פרטי טביעות האצבע אינם נשמרים עד ללחיצה על **Next** (הבא). אם תשאיר את המחשב ללא כל פעילות למשך זמן מה, או אם תסגור את התוכנית, השינויים שביצעת **לא** יישמרו.

רישום סצינות

עליך לרשום סצינה אחת או יותר כדי להשתמש בכניסה באמצעות זיהוי הפנים.

לרישום סצינה חדשה מאשף ההתקנה של HP ProtectTools Security Manager:

1. לחץ על הסמל **HP ProtectTools Security Manager** בסרגל הצידי שבצידו הימני או השמאלי של המסך.

2. הזן את סיסמת Windows® ולאחר מכן לחץ על **Next** (הבא).

3. תחת **Enable security features** (הפעל מאפייני אבטחה), בחר בתיבת הסימון **Windows Logon Security** (אבטחת הכניסה של Windows) ולאחר מכן לחץ על **Next** (הבא).

4. תחת **Choose your credentials** (בחירת ההרשאה), בחר בתיבת הסימון **Face** (פנים) ולאחר מכן לחץ על **Next** (הבא).

5. לחץ על **Enroll a new scene** (רישום סצינה חדשה).

לאחר שהרישום הושלם בהצלחה, באפשרותך גם לרשום סצינה חדשה אם נתקלת בבעיה במהלך הכניסה מכיוון שלפחות אחד מהתנאים הבאים השתנה:

- פניך השתנו באופן משמעותי מאז הרישום האחרון.
- התאורה שונה למדי בהשוואה לרישומים האחרונים שלך.
- במהלך הרישום האחרון, הרכבת משקפיים (או שלא).

> **הערה:** אם אתה מתקשה ברישום סצינות, נסה להתקרב למצלמת האינטרנט. כמו בכל סוג של צילום או וידאו, יש חשיבות רבה לתאורה ולניגודיות. ודא שהתאורה במקום הצילום נמצאת בעיקר בחלק הקדמי ולא בחלק האחורי. אם Face Recognition (זיהוי הפנים) לא מאמת אותך, ייתכן שתרצה לבצע רישום מחדש של הסצינה עם תאורה משופרת.

לרישום סצינה חדשה מ-HP ProtectTools Security Manager:

1. לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), לחץ על **HP** ולאחר מכן לחץ על **HP ProtectTools Security Manager**.
2. לחץ על **Credentials** (הרשאות) ולאחר מכן לחץ על **Face** (פנים).
3. לחץ על **Enroll a new scene** (רישום סצינה חדשה).

הגדרות מתקדמות למשתמש

1. לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), ולאחר מכן לחץ על **HP ProtectTools Security Manager**.
2. לחץ על **Set up your authentication credentials** (הגדרת הרשאות האימות), ולאחר מכן לחץ על **Face** (פנים).
3. לחץ על לחצן **Advanced** (מתקדם), ולאחר מכן בחר מהאפשרויות הבאות.

א. לצורך השימוש ב-PIN לכניסה באמצעות זיהוי הפנים, לחץ על **Create PIN** (יצירת PIN), הזן את סיסמת Windows, הזן את ה-PIN החדש, ולאחר מכן אשר אותו באמצעות הזנתו מחדש.

ב. בחר הגדרות נוספות, אם רצונך בכך. הגדרות אלה מתייחסות למשתמש הנוכחי בלבד:

- **הפעלת קול באירועי זיהוי הפנים**
  - בחר את תיבת הסימון להפעלת קול כשזיהוי הפנים מצליח או נכשל.
  - בטל את הסימון בתיבת הסימון כדי להשבית אפשרות זו.
- **הנחיה לעדכן סצינות בעת כשל בזיהוי**
  - בחר את תיבת הסימון כדי לאפשר למשתמש לעדכן סצינות אם זיהוי הפנים נכשל. אם האימות מגיע לסף "אולי", המשתמש מתבקש להחליט אם להזין את התמונות בזמן אמת בכניסה ש"נכשלה" לסצינה הנוכחית כדי להגדיל את הסיכוי לכניסה מוצלחת בפעם הבאה.
  - בטל את הסימון בתיבת הסימון כדי להשבית אפשרות זו.
- **הנחיה לרשום סצינה חדשה בעת כשל בכניסה**
  - בחר את תיבת הסימון כדי להציג הנחיה המורה למשתמש לרשום סצינה חדשה אם זיהוי הפנים נכשל והאימות אינו מגיע לסף "אולי". ייתכן שפעולה זו תגדיל את הסיכוי לכניסה מוצלחת בפעם הבאה.
  - בטל את הסימון בתיבת הסימון כדי להשבית אפשרות זו.

ג. לרישום סצינה חדשה, לחץ על **Enroll a new scene** (רישום סצינה חדשה) ולאחר מכן פעל על-פי ההוראות שעל-גבי המסך.

שינוי סיסמת Windows

Security Manager (מנהל האבטחה) הופך את שינוי סיסמת Windows לפשוט ומהיר יותר מאשר באמצעות לוח הבקרה של Windows.

כדי לשנות את סיסמת Windows, בצע את השלבים הבאים:

1. מלוח המחוונים של Security Manager (מנהל האבטחה), לחץ על **Credentials** (הרשאות) ולאחר מכן לחץ על **Password** (סיסמה).
2. הזן את הסיסמה הנוכחית בתיבת הטקסט **Current Windows password** (סיסמת Windows נוכחית).

3. הקלד סיסמה חדשה בתיבת הטקסט **New Windows password** (סיסמת Windows חדשה), ולאחר מכן הקלד אותה שוב בתיבת הטקסט **Confirm new password** (אישור סיסמה חדשה).
4. לחץ על **Change** (שנה) כדי לשנות את הסיסמה הנוכחית לסיסמה החדשה שהזנת באופן מיידי.

הגדרת כרטיס חכם

אם בחרת בכניסה באמצעות כרטיס חכם ואם קורא כרטיסים חכמים מובנה במחשב או מחובר אליו, אשף ההתקנה של Security Manager ינחה אותך להגדיר PIN (מספר זיהוי אישי) של כרטיס חכם.

כדי להגדיר PIN של כרטיס חכם:

1. בדף **Set up smart card** (הגדרת כרטיס חכם), הזן ואשר מספר PIN.

   באפשרותך גם לשנות את ה-PIN. הזן את ה-PIN הנוכחי שלך ולאחר מכן הזן PIN חדש.
2. להמשך, לחץ על **Next** (הבא) ולאחר מכן עקוב אחר ההוראות שעל-גבי המסך.

- לחלופין -

▲ מלוח המחוונים של Security Manager (מנהל האבטחה), לחץ על **Credentials** (הרשאות) ולאחר מכן לחץ על **Smart Card** (כרטיס חכם).

- כדי להגדיר PIN של כרטיס חכם—תחת בדף **Set up smart card** (הגדרת כרטיס חכם), הזן ואשר את ה-PIN.
- כדי לשנות את ה-PIN—הקלד תחילה את ה-PIN הנוכחי ולאחר מכן אשר את ה-PIN החדש.

משימות כלליות

היישומים הכלולים בקבוצה זו מסייעים בניהול היבטים שונים של הזהות הדיגיטלית שלך.

- **Security Manager** (מנהל האבטחה)—היישום יוצר ומנהל קישורים מהירים, המאפשרים לך להפעיל אתרי אינטרנט ותוכניות ולהיכנס אליהם על-ידי אימות באמצעות סיסמת Windows, טביעת אצבע או כרטיס חכם.
- **Credentials** (הרשאות)—היישום מספק אמצעי לשינוי קל של סיסמת Windows, רישום טביעות אצבע או הגדרת כרטיס חכם.

כדי להוסיף יישומים נוספים, לחץ על הלחצן **Discover more** [+] (גלה עוד) בפינה השמאלית או הימנית התחתונה בלוח המחוונים. ייתכן שמנהל המערכת השבית לחצן זה.

Password Manager (מנהל הסיסמאות)

הכניסה ל-Windows, אתרי אינטרנט ויישומים קלה ובטוחה יותר בעת השימוש ב-Password Manager (מנהל הסיסמאות). באפשרותך להשתמש בו ליצירת סיסמאות חזקות יותר שאינך חייב לכתוב או לזכור, ולאחר מכן להיכנס בקלות ובמהירות באמצעות טביעת אצבע, כרטיס חכם או סיסמת Windows.

Password Manager (מנהל הסיסמאות) מציע את האפשרויות הבאות:

- הוסף, ערוך או מחק פרטי כניסה מהכרטיסייה Manage (ניהול).
- השתמש בקישורים מהירים להפעלת דפדפן ברירת המחדל ולכניסה לאתר אינטרנט או תוכנית כלשהם לאחר ההגדרה.
- גרור ושחרר כדי לסדר את הקישורים המהירים בקטגוריות.
- בדוק במהירות אם סיסמה כלשהי מהווה סיכון בטיחותי והפק סיסמה חזקה ומורכבת באופן אוטומטי לשימוש באתרים חדשים.

מאפיינים רבים של Password Manager זמינים גם מסמל מנהל הסיסמאות המוצג כאשר המוקד נמצא במסך הכניסה של דף אינטרנט או תוכנית. לחץ על הסמל כדי להציג תפריט הקשר שבו תוכל לבחור מבין האפשרויות הבאות.

עבור דפי אינטרנט או תוכניות שבהם לא נוצרו עדיין פרטי כניסה

האפשרויות הבאות מוצגות בתפריט ההקשר:

- **Add [somedomain.com] to the Password Manager** (הוסף את [somedomain.com] למנהל הסיסמאות)—האפשרות מאפשרת לך להוסיף פרטי כניסה עבור מסך הכניסה הנוכחי.
- **Open Password Manager** (פתח את מנהל הסיסמאות)—האפשרות מפעילה את Password Manager.
- **Icon settings** (הגדרות סמל)—האפשרות מאפשרת לך לציין תנאים להצגת סמל Password Manager (מנהל הסיסמאות).
- **Help** (עזרה)—האפשרות מציגה את עזרת התוכנה של Password Manager.

עבור דפי אינטרנט או תוכניות שבהם כבר נוצרו פרטי כניסה

האפשרויות הבאות מוצגות בתפריט ההקשר:

- **Fill in logon data** (מלא נתוני כניסה)—האפשרות מציבה את נתוני הכניסה בשדות הכניסה ושולחת את הדף (אם צוינה שליחה בעת היצירה או העריכה האחרונה של פרטי הכניסה).
- **Edit logon** (ערוך פרטי כניסה)—האפשרות מאפשרת לך לערוך את נתוני הכניסה עבור אתר אינטרנט זה.
- **Add a New Account** (הוסף חשבון חדש)—האפשרות מאפשרת לך להוסיף חשבון לכניסה.

- **Open Password Manager** (פתח את מנהל הסיסמאות)—האפשרות מפעילה את היישום Password Manager.
- **Help** (עזרה)—האפשרות מציגה את עזרת התוכנה של Password Manager.

הערה: ייתכן שמנהל המערכת של מחשב זה הגדיר את Security Manager (מנהל האבטחה) לדרוש יותר מהרשאה אחת בעת אימות זהותך.

הוספת פרטי כניסה

באפשרותך להוסיף פרטי כניסה בקלות עבור אתר אינטרנט או תוכנית על-ידי הזנת מידע הכניסה פעם אחת. לאחר מכן, Password Manager יזין את המידע עבורך באופן אוטומטי. באפשרותך להשתמש בפרטי כניסה אלה לאחר הגלישה אל אתר האינטרנט או התוכנית, או ללחוץ על פרטי כניסה מתפריט **Logons** (פרטי כניסה) כדי לגרום ל-Password Manager לפתוח את אתר האינטרנט או התוכנית ולהכניס אותך אליהם.

כדי להוסיף פרטי כניסה:

1. פתח את מסך הכניסה של אתר אינטרנט או תוכנית כלשהם.
2. לחץ על החץ בסמל **Password Manager** (מנהל הסיסמאות) ולאחר מכן לחץ על אחת מהאפשרויות הבאות, בהתאם לשיוכו של מסך הכניסה לאתר אינטרנט או לתוכנית:
   - עבור אתר אינטרנט, לחץ על **Add [domain name] to Password Manager** (הוסף את [שם תחום] למנהל הסיסמאות).
   - עבור תוכנית, לחץ על **Add this logon screen to Password Manager** (הוסף מסך כניסה זה למנהל הסיסמאות).
3. הזן את נתוני הכניסה. שדות כניסה במסך, והשדות התואמים בתיבת הדו-שיח, מזוהים על-ידי גבול כתום בולט. ניתן גם להציג תיבת דו-שיח זו על-ידי לחיצה על **Add Logon** (הוסף כניסה) מהכרטיסייה **Manage** (ניהול) של Password Manager. אפשרויות מסוימות תלויות בהתקני האבטחה המחוברים למחשב; לדוגמה, שימוש במקש החם ctrl+Windows+h, סריקת טביעות אצבע או הכנסת כרטיס חכם.

   א. כדי לאכלס את שדה הכניסה באחת מהאפשרויות המוגדרות מראש, לחץ על החצים משמאל או מימין לשדה.

   ב. כדי להציג את הסיסמה עבור כניסה זו, לחץ על **Show password** (הצג סיסמה).

   ג. כדי למלא את שדות הכניסה, אך לא לשלוח אותם, נקה את תיבת הסימון **Automatically submit logon data** (שלח נתוני כניסה באופן אוטומטי).

   ד. לחץ על **OK** (אישור), לחץ על שיטת האימות שברצונך להשתמש בה: **Fingerprints** (טביעות אצבע), **Password** (סיסמה), או **Face** (פנים), ולאחר מכן התחבר באמצעות שיטת האימות שבחרת.

   סימן החיבור יוסר מסמל Password Manager (מנהל הסיסמאות) כדי להודיע לך שהכניסה נוצרה.

   ה. אם Password Manager (מנהל הסיסמאות) אינו מזהה את שדות הכניסה, לחץ על **More fields** (שדות נוספים).

      i. בחר את תיבת הסימון עבור כל שדה הנדרש לכניסה או נקה את תיבת הסימון משדות שאינם נדרשים לכניסה.

      ii. אם Password Manager (מנהל הסיסמאות) אינו יכול לזהות את כל שדות הכניסה, תופיע הודעה השואלת אם ברצונך להמשיך. לחץ על **Yes** (כן).

      iii. תופיע תיבת דו-שיח עם שדות הכניסה הכוללים פרטים מלאים. לחץ על הסמל עבור כל שדה וגרור אותו לשדה הכניסה המתאים ולאחר מכן לחץ על הלחצן כדי להיכנס לאתר האינטרנט.

הערה: לאחר השימוש במצב הידני של הזנת נתוני הכניסה עבור אתר, עליך להמשיך להשתמש בשיטה זו כדי שבעתיד תוכל להיכנס לאותו אתר האינטרנט.

הערה: המצבר הידני של הזנת נתוני הכניסה זמין רק ב-Internet Explorer 8.

iv. לחץ על **Close** (סגור).

בכל פעם שאתה ניגש לאותו אתר אינטרנט או פותח את אותה תוכנית, סמל Password Manager (מנהל הסיסמאות) מוצג ומציין שבאפשרותך להשתמש בהרשאות הרשומות לצורך הכניסה.

עריכת פרטי כניסה

כדי לערוך כניסה, בצע את השלבים הבאים:

1. פתח את מסך הכניסה של אתר אינטרנט או תוכנית כלשהם.
2. כדי להציג תיבת דו-שיח שבה תוכל לערוך את מידע הכניסה, לחץ על החץ בסמל **Password Manager** (מנהל הסיסמאות) ולאחר מכן לחץ על **Edit logon** (ערוך כניסה). שדות כניסה במסך, והשדות התואמים בתיבת הדו-שיח, מזוהים על-ידי גבול כתום בולט.

   ניתן גם להציג תיבת דו-שיח זו על-ידי לחיצה על **Edit for the desired logon** (עריכה עבור הכניסה הרצויה) בכרטיסייה **Manage** (ניהול) של Password Manager (מנהל הסיסמאות).
3. ערוך את מידע הכניסה.
   - כדי לאכלס את שדה הכניסה באחת מהאפשרויות המוגדרות מראש, לחץ על החצים משמאל או מימין לשדה.
   - כדי להוסיף שדות נוספים מהמסך לפרטי הכניסה, לחץ על **More fields** (שדות נוספים).
   - כדי למלא את שדות הכניסה, אך לא לשלוח אותם, נקה את תיבת הסימון **Submit logon data** (שלח נתוני כניסה).
   - כדי להציג את הסיסמה עבור כניסה זו, לחץ על **Show password** (הצג סיסמה).
4. לחץ על **OK** (אישור).

שימוש בתפריט Logons (פרטי כניסה)

Password Manager (מנהל הסיסמאות) מספק דרך מהירה וקלה להפעלת אתרי האינטרנט והתוכניות שעבורם יצרת פרטי כניסה. לחץ לחיצה כפולה על כניסה של תוכנית או אתר אינטרנט מתפריט **Logons** (פרטי כניסה), או בכרטיסייה **Manage** (ניהול) ב-**Password Manager** (מנהל הסיסמאות), כדי לפתוח את מסך הכניסה ולמלא את נתוני הכניסה.

בעת יצירת כניסה, היא נוספת באופן אוטומטי לתפריט Logons (פרטי כניסה) של Password Manager (מנהל הסיסמאות).

כדי להציג את תפריט Logons (פרטי כניסה):

1. הקש את שילוב המקשים החם של **Password Manager**. ctrl+Windows+h הוא הגדרת היצרן. כדי לשנות את שילוב המקשים החם, לחץ על **Password Manager** ולאחר מכן לחץ על **Settings** (הגדרות).
2. סרוק את טביעת האצבע שלך (במחשבים עם קורא טביעות אצבע מובנה או מחובר).

סידור פרטי כניסה בקטגוריות

השתמש בקטגוריות לשמירה על הסדר בפרטי הכניסה על-ידי יצירת קטגוריה אחת או יותר. לאחר מכן גרור ושחרר את פרטי הכניסה בקטגוריות הרצויות.

כדי להוסיף קטגוריה:

1. מלוח המחוונים של Security Manager (מנהל האבטחה), לחץ על **Password Manager** (מנהל הסיסמאות).
2. לחץ על הכרטיסייה **Manage** (ניהול) ולאחר מכן לחץ על **Add Category** (הוסף קטגוריה).

3. הזן שם עבור הקטגוריה.
4. לחץ על **OK** (אישור).

כדי להוסיף כניסה לקטגוריה:

1. הצב את מצביע העכבר מעל לכניסה הרצויה.
2. לחץ ממושכות על לחצן העכבר השמאלי.
3. גרור את הכניסה אל רשימת הקטגוריות. הקטגוריות יודגשו עם המעבר מעליהן עם העכבר.
4. שחרר את לחצן העכבר בעת הדגשת הקטגוריה הרצויה.

פרטי הכניסה אינם מועברים אלא רק מועתקים לקטגוריה שנבחרה. באפשרותך להוסיף את אותה הכניסה ליותר מקטגוריה אחת, ובאפשרותך להציג את כל פרטי הכניסה על-ידי לחיצה על **All** (הכל).

ניהול פרטי הכניסה

Password Manager (מנהל הסיסמאות) מקל עליך לנהל את מידע הכניסה, כגון שמות משתמש, סיסמאות וחשבונות כניסה מרובים, ממיקום מרכזי אחד.

פרטי הכניסה רשומים בכרטיסייה Manage (ניהול). אם נוצרו פרטי כניסה מרובים עבור אותו אתר אינטרנט, כל כניסה תירשם תחת שם אתר האינטרנט ותזוז פנימה ברשימת פרטי הכניסה.

כדי לנהל את פרטי הכניסה:

מלוח המחוונים של Security Manager (מנהל האבטחה), לחץ על **Password Manager** (מנהל הסיסמאות) ולאחר מכן לחץ על הכרטיסייה **Manage** (ניהול).

- **הוספת כניסה**—לחץ על **Add Logon** (הוסף כניסה) ופעל בהתאם להוראות על המסך.
- **עריכת כניסה**—לחץ על כניסה, לחץ על **Edit** (ערוך) ולאחר מכן שנה את נתוני הכניסה.
- **מחיקת כניסה**—לחץ על כניסה ולאחר מכן לחץ על **Delete** (מחק).

כדי להוסיף כניסה נוספת עבור אתר אינטרנט או תוכנית:

1. פתח את מסך הכניסה של אתר האינטרנט או התוכנית.
2. לחץ על סמל **Password manager** (מנהל הסיסמאות) כדי להציג את תפריט הקיצור שלו.
3. לחץ על **Add additional logon** (הוסף כניסה נוספת) ולאחר מכן פעל בהתאם להוראות על המסך.

הערכת עוצמת הסיסמה

השימוש בסיסמאות חזקות לכניסה לאתרי אינטרנט ותוכניות הוא היבט חשוב בהגנה על זהותך.

Password Manager (מנהל הסיסמאות) מקל על הניטור והשיפור של האבטחה באמצעות ניתוח מיידי ואוטומטי של העוצמה של כל אחת מהסיסמאות המשמשות לכניסה לאתרי האינטרנט והתוכניות שלך.

הגדרות סמל Password Manager (מנהל הסיסמאות)

Password Manager (מנהל הסיסמאות) מנסה לזהות מסכי כניסה של אתרי אינטרנט ותוכניות. כאשר הוא מזהה מסך כניסה שעדיין לא יצרת עבורו כניסה, Password Manager (מנהל הסיסמאות) מנחה אותך להוסיף כניסה עבור המסך על-ידי הצגת סמל Password Manager עם סימן +.

לחץ על חץ הסמל ולאחר מכן לחץ על **Icon Settings** (הגדרות סמל) כדי להתאים אישית את האופן שבו **Password Manager** (מנהל הסיסמאות) מטפל באתרי כניסה אפשריים.

- **Prompt to add logons for logon screens** (הצג בקשה להוספת פרטי כניסה עבור מסכי כניסה)—לחץ על אפשרות זו כדי לגרום ל-Password Manager (מנהל הסיסמאות) לבקש ממך להוסיף כניסה בעת הצגת מסך כניסה שעדיין לא הוגדרה בו כניסה.
- **Exclude this screen** (אל תכלול מסך זה)—בחר את תיבת הסימון כדי ש-Password Manager לא יבקש ממך שוב להוסיף כניסה עבור מסך כניסה זה.

כדי לגשת להגדרות נוספות של Password Manager (מנהל הסיסמאות), לחץ על **Password Manager** ולאחר מכן לחץ על **Settings** (הגדרות) בלוח המחוונים של Security Manager (מנהל האבטחה).

הגדרות

באפשרותך לציין הגדרות להתאמה אישית של HP ProtectTools Security Manager:

1. **Prompt to add logons for logon screens** (הצג בקשה להוספת פרטי כניסה עבור מסכי כניסה)—סמל Password Manager (מנהל הסיסמאות) עם סימן חיבור מוצג בכל פעם שמזוהה מסך כניסה של אתר אינטרנט או תוכנית, כדי לציין שבאפשרותך להוסיף כניסה עבור מסך זה לכספת הסיסמאות. כדי להשבית מאפיין זה, בתיבת הדו-שיח **Icon Settings** (הגדרות סמל), נקה את תיבת הסימון מחוץ ל-**Prompt to add logons for logon screens** (הצג בקשה להוספת פרטי כניסה עבור מסכי כניסה).
2. **Open Password Manager with ctrl+Windows+h** (פתח את Password Manager באמצעות ctrl +Windows+h)—המקש החם המוגדר כברירת מחדל אשר פותח את תפריט Quick Links (קישורים מהירים) של Password Manager הוא ctrl+Windows+h. כדי לשנות את המקש החם, לחץ על אפשרות זו והזן שילוב מקשים חדש. השילובים יכולים לכלול אחד או יותר מהמקשים הבאים: ctrl, alt או shift וכל מקש אלפביתי או מספרי.
3. לחץ על **Apply** (החל) כדי לשמור את השינויים.

הרשאות

יש להשתמש בהרשאות של Security Manager (מנהל האבטחה) כדי לאמת את זהותך. מנהל המערכת המקומי של מחשב זה יכול להגדיר את ההרשאות שישמשו להוכחת זהותך בעת הכניסה לחשבון Windows, לאתרי אינטרנט או לתוכניות.

ההרשאות הזמינות משתנות בהתאם להתקני האבטחה המובנים במחשב או המחוברים אליו. עבור כל הרשאה נתמכת מופיעה רשומה בקבוצה **My Identity, Credentials** (הזהות שלי, הרשאות).

הרשאות זמינות, דרישות ומצב נוכחי מפורטים ועשויים לכלול את הפריטים הבאים:

- טביעות אצבע
- סיסמה
- כרטיס חכם
- פנים

כדי לרשום או לשנות הרשאה, לחץ על הקישור ופעל בהתאם להוראות על המסך.

כרטיס הזיהוי האישי שלך

כרטיס הזיהוי שלך מזהה אותך באופן ייחודי כבעלים של חשבון Windows זה, והוא מציג את שמך ותמונה לפי בחירתך. הוא מוצג לצמיתות בפינה השמאלית או הימנית העליונה של דפי Security Manager (מנהל האבטחה) וכאביזר של הסרגל הצידי של Windows.

לחיצה על כרטיס הזיהוי בסרגל הצידי של Windows היא אחת מהדרכים הרבות לגשת במהירות ל-Security Manager (מנהל האבטחה).

באפשרותך לשנות את התמונה ואת האופן שבו שמך מוצג. כברירת מחדל, מוצגים שם המשתמש המלא של Windows והתמונה שבחרת במהלך הגדרת Windows.

כדי לשנות את השם המוצג:

1. מלוח המחוונים של Security Manager (מנהל האבטחה), לחץ על הסמל **ID Card** (כרטיס הזיהוי) בפינה השמאלית או הימנית העליונה.
2. לחץ על תיבת הסימון המציגה את השם שהזנת עבור החשבון שלך ב-Windows. המערכת תציג את שם המשתמש של Windows עבור חשבון זה.
3. כדי לשנות שם זה, הקלד את השם החדש ולאחר מכן לחץ על הלחצן **Save** (שמור).

כדי לשנות את התמונה המוצגת:

1. מלוח המחוונים של Security Manager (מנהל האבטחה), לחץ על **ID Card** (כרטיס הזיהוי) בפינה השמאלית או הימנית העליונה.
2. לחץ על הלחצן **Choose picture** (בחר תמונה), לחץ על תמונה ולאחר מכן לחץ על הלחצן **Save** (שמור).

הגדרת ההעדפות שלך

באפשרותך להתאים אישית את ההגדרות של HP ProtectTools Security Manager. מלוח המחוונים של Security Manager, לחץ על **Advanced** (מתקדם) ולאחר מכן לחץ על **Preferences** (העדפות). ההגדרות הזמינות מוצגות בשתי כרטיסיות: General (כללי) ו-Fingerprint (טביעת אצבע).

General (כללי)

ההגדרות הבאות זמינות בכרטיסייה General (כללי):

Appearance (מראה)—**Show icon on taskbar** (הצג סמל בשורת המשימות)

- כדי לאפשר את הצגת הסמל בשורת המשימות, בחר את תיבת הסימון.
- כדי להשבית את הצגת הסמל בשורת המשימות, נקה את תיבת הסימון.

Fingerprint (טביעת אצבע)

ההגדרות הבאות זמינות בכרטיסייה Fingerprint (טביעת אצבע):

- **Quick Actions** (פעולות מהירות)—השתמש בפעולות מהירות כדי לבחור את משימת Security Manager לביצוע בעת לחיצה ממושכת על המקש המיועד בעת סריקת טביעת האצבע שלך.

  כדי להקצות פעולה מהירה לאחד מהמקשים הרשומים, לחץ על האפשרות **(Key) + Fingerprint** ((מקש) +טביעת אצבע) ולאחר מכן בחר באחת המשימות הזמינות מתוך התפריט.

- **Fingerprint Scan Feedback** (משוב של סריקת טביעת אצבע)—האפשרות מוצגת רק כאשר קורא טביעות אצבע זמין. השתמש בהגדרה זו כדי לכוונן את המשוב שמתרחש בעת סריקת טביעת האצבע.

  - **Enable sound feedback** (הפעל משוב קולי)—Security Manager מספק משוב שמע בעת סריקה של טביעת אצבע, ומשמיע צלילים שונים עבור אירועי תוכנית ספציפיים. באפשרותך להקצות צלילים חדשים לאירועים אלה באמצעות הכרטיסייה Sounds (צלילים) בלוח הבקרה של Windows, או להשבית משוב קולי על-ידי ניקוי האפשרות.

  - **Show scan quality feedback (הצג משוב של איכות הסריקה)**

    להצגת כל הסריקות, ללא קשר לאיכות, בחר את תיבת הסימון.

    להצגת סריקות באיכות טובה בלבד, נקה את תיבת הסימון.

גיבוי ושחזור של הנתונים

מומלץ לגבות את נתוני Security Manager (מנהל האבטחה) באופן קבוע. תדירות הגיבוי תלויה בתדירות שינוי הנתונים. לדוגמה, אם אתה מוסיף פרטי כניסה חדשים מדי יום, כדאי לגבות את הנתונים מדי יום.

ניתן גם להשתמש בגיבויים לביצוע העברה ממחשב אחד לאחר, פעולה הנקראת גם יבוא וייצוא.

הערה: מאפיין זה מגבה נתונים בלבד.

יש להתקין את HP ProtectTools Security Manager בכל מחשב שאמור לקבל נתונים מגובים לפני שניתן יהיה לשחזר את הנתונים מקובץ הגיבוי.

כדי לגבות את הנתונים:

1. בלוח השמאלי או הימני, לחץ על **Advanced** (מתקדם) ולאחר מכן לחץ על **Backup and Restore** (גיבוי ושחזור).
2. לחץ על **Back up data** (גבה נתונים).
3. בחר את המודולים שברצונך לכלול בגיבוי. ברוב המקרים, כדאי לבחור את כולם.
4. הזן שם עבור קובץ האחסון. כברירת מחדל, הקובץ יישמר בתיקייה Documents (מסמכים). לחץ על **Browse** (עיון) כדי לציין מיקום אחר.
5. הזן סיסמה להגנה על הקובץ.
6. אמת את זהותך.
7. לחץ על **Finish** (סיום).

כדי לשחזר את הנתונים:

1. בלוח השמאלי או הימני, לחץ על **Advanced** (מתקדם) ולאחר מכן לחץ על **Backup and Restore** (גיבוי ושחזור).
2. לחץ על **Restore data** (שחזר נתונים).

3. בחר את קובץ האחסון שנוצר קודם. באפשרותך להזין את הנתיב בשדה שמופיע או ללחוץ על **Browse** (עיון).
4. הזן את הסיסמה המשמשת להגנה על הקובץ.
5. בחר את המודולים שאת הנתונים שלהם ברצונך לשחזר. ברוב המקרים, מדובר בכל המודולים ברשימה.
6. לחץ על **Finish** (סיום).

Discover more (גלה עוד)

ייתכן שזמינים יישומים נוספים המספקים מאפיינים חדשים עבור תוכנית זו.

מלוח המחוונים של Security Manager, לחץ על **Discover more [+]** (גלה עוד) כדי לעיין ביישומים נוספים.

הערה: אם אין קישור מסוג **Discover more [+]** בחלק השמאלי או הימני העליון של לוח המחוונים, הוא הושבת על-ידי מנהל המערכת של מחשב זה.

עדכונים והודעות

1. כדי לבקש מידע לגבי יישומים ועדכונים חדשים, בחר בתיבת הסימון **ברצוני לקבל הודעות לגבי יישומים ועדכונים חדשים.**
2. כדי להגדיר תזמון עבור עדכונים אוטומטיים, בחר את מספר הימים.
3. כדי לחפש עדכונים, לחץ על **Check Now** (בדוק כעת).

מצב יישומי אבטחה

הדף Security Manager Applications Status (מצב יישומי מנהל האבטחה) מציג את המצב הכולל של יישומי האבטחה המותקנים. הדף מציג את היישומים המוגדרים ואת מצב ההגדרה של כל אחד מהם. הסיכום מוצג באופן אוטומטי בעת פתיחת לוח המחוונים של Security Manager (מנהל האבטחה), או בעת לחיצה על **Check the status of the security applications** (בדיקת המצב של יישומי האבטחה), בעת לחיצה על **Security Applications** (יישומי אבטחה), או בעת לחיצה על **Check Now** (בדוק כעת) בסמל **Gadget** (גאדג'ט), בסרגל הצידי של Windows בצידו הימני או השמאלי של המסך.

8 Drive Encryption for HP ProtectTools (בדגמים נבחרים בלבד)

זהירות: אם תחליט להסיר את התקנת המודול Drive Encryption (הצפנת כונן), תחילה עליך לבטל את ההצפנה של כל הכוננים המוצפנים. אם לא תבטל את הצפנת הכוננים, לא תוכל לגשת לנתונים בכוננים מוצפנים אלא אם כן ביצעת רישום בשירות השחזור של Drive Encryption (הצפנת כונן). התקנה מחדש של המודול Drive Encryption (הצפנת כונן) לא תאפשר לך לגשת לכוננים מוצפנים.

Drive Encryption for HP ProtectTools מספק הגנה מלאה על נתונים על-ידי הצפנת הכונן הקשיח של המחשב. כאשר Drive Encryption (הצפנת כונן) מופעל, עליך להיכנס דרך מסך הכניסה של Drive Encryption (הצפנת כונן) המוצג לפני האתחול של מערכת ההפעלה של ®Windows.

אשף ההתקנה של HP ProtectTools מאפשר למנהלי מערכת של Windows להפעיל את Drive Encryption (הצפנת כונן), לגבות את מפתח ההצפנה, להוסיף ולהסיר משתמשים ולהשבית את Drive Encryption (הצפנת כונן). עיין בעזרה של תוכנת HP ProtectTools Security Manager לקבלת מידע נוסף.

ניתן לבצע את המשימות הבאות באמצעות Drive Encryption (הצפנת כונן):

- ניהול הצפנה

  הצפנה או פענוח של כוננים בודדים

הערה: ניתן להצפין כוננים קשיחים פנימיים בלבד.

- שחזור
  - יצירת מפתחות גיבוי
  - ביצוע שחזור

הליכי הגדרה

פתיחת Drive Encryption (הצפנת כונן)

1. לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), לחץ על **HP** ולאחר מכן לחץ על **HP ProtectTools Administrative Console**.
2. בחלונית השמאלית או הימנית, לחץ על **Drive Encryption** (הצפנת כונן).

משימות כלליות

הפעלת Drive Encryption (הצפנת כונן)

השתמש באשף ההתקנה של HP ProtectTools להפעלת Drive Encryption (הצפנת כונן).

הערה: אשף זה משמש גם להוספה ולהסרה של משתמשים.

- לחלופין -

1. לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), לחץ על **HP** ולאחר מכן לחץ על **HP ProtectTools Administrative Console**.
2. בחלונית השמאלית או הימנית, לחץ על **Security** (אבטחה) ולאחר מכן לחץ על **Features** (מאפיינים).
3. בחר את תיבת הסימון **Drive Encryption** (הצפנת כונן) ולאחר מכן לחץ על **Next** (הבא).
4. תחת **Drives to be encrypted** (כוננים להצפנה), בחר את תיבת הסימון של הכונן הקשיח שברצונך להצפין.
5. הכנס את התקן האחסון לחריץ המתאים.

   הערה: כדי לשמור את מפתח ההצפנה, עליך להשתמש בהתקן אחסון מסוג USB עם תבנית FAT32.

6. תחת **External storage device on which to save encryption key** (התקן אחסון חיצוני שבו יש לשמור מפתח הצפנה), בחר את תיבת הסימון של התקן האחסון שבו יישמר מפתח ההצפנה.
7. לחץ על **Apply** (החל).

   הצפנת הכונן מתחילה.

עיין בעזרה של תוכנת HP ProtectTools Security Manager לקבלת מידע נוסף.

השבתת Drive Encryption (הצפנת כונן)

השתמש באשף ההתקנה של HP ProtectTools להשבתת Drive Encryption (הצפנת כונן). עיין בעזרה של תוכנת HP ProtectTools Security Manager לקבלת מידע נוסף.

- לחלופין -

1. לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), לחץ על **HP** ולאחר מכן לחץ על **HP ProtectTools Administrative Console**.
2. בחלונית השמאלית או הימנית, לחץ על **Security** (אבטחה) ולאחר מכן לחץ על **Features** (מאפיינים).
3. נקה את תיבת הסימון **Drive Encryption** (הצפנת כונן) ולאחר מכן לחץ על **Apply** (החל).

   פענוח הכונן מתחיל.

כניסה לאחר הפעלת Drive Encryption (הצפנת כונן)

בעת הפעלת המחשב לאחר הפעלת Drive Encryption (הצפנת כונן) כאשר חשבון המשתמש שלך רשום, עליך להיכנס דרך מסך הכניסה של Drive Encryption (הצפנת כונן):

הערה: אם מנהל המערכת של Windows אפשר אבטחת טרום-אתחול ב-HP ProtectTools Security Manager, תיכנס למחשב באופן מיידי לאחר הפעלת המחשב במקום להגיע למסך הכניסה של Drive Encryption (הצפנת כונן).

1. לחץ על שם המשתמש שלך ולאחר מכן הקלד את סיסמת Windows או ה-PIN של Java™ Card, או העבר אצבע שרשמת את טביעתה.
2. לחץ על **OK** (אישור).

הערה: אם אתה משתמש במפתח שחזור לכניסה דרך מסך הכניסה של Drive Encryption (הצפנת כונן), תתבקש גם לבחור את שם המשתמש של Windows ולהקליד את הסיסמה שלך במסך הכניסה של Windows.

הגנה על הנתונים על-ידי הצפנת הכונן הקשיח

השתמש באשף ההתקנה של HP ProtectTools כדי להגן על הנתונים על-ידי הצפנת הכונן הקשיח:

1. ב-Security Manager, לחץ על **Getting Started** (תחילת העבודה) ולאחר מכן לחץ על סמל **Security Manager Setup** (הגדרת מנהל האבטחה). הדגמה המתארת את מאפייני Security Manager מתחילה. (ניתן גם להפעיל את Security Manager מהדף Drive Encryption.)
2. בחלונית השמאלית או הימנית, לחץ על **Drive Encryption** (הצפנת כונן) ולאחר מכן לחץ על **Encryption Management** (ניהול הצפנה).
3. לחץ על **Change Encryption** (שינוי הצפנה).
4. בחר את הכונן או הכוננים להצפנה.

הערה: מומלץ מאוד להצפין את הכונן הקשיח.

הצגת מצב הצפנה

למשתמשים יש אפשרות להציג מצב הצפנה מתוך HP ProtectTools Security Manager.

הערה: יש לבצע שינויים במצב הצפנת הכונן באמצעות HP ProtectTools Administrative Console.

1. פתח את **HP ProtectTools Security Manager**.
2. תחת **My Data** (הנתונים שלי), לחץ על **Encryption Status** (מצב הצפנה).

אם המאפיין Drive Encryption (הצפנת כונן) פעיל, מצב הכונן מציג את אחד מקודי המצב הבאים:

- Active (פעיל)
- Inactive (לא פעיל)
- Not encrypted (לא מוצפן)
- Encrypted (מוצפן)
- Encrypting (מצפין)
- Decrypting (מפענח)

אם הכונן הקשיח נמצא בתהליך של הצפנה או פענוח, סרגל התקדמות מציג את אחוז הביצוע והזמן הנותר להשלמת ההצפנה או הפענוח.

משימות מתקדמות

ניהול ה-Drive Encryption (הצפנת כונן) (משימה של מנהל מערכת)

הדף Encryption Management (ניהול הצפנה) מאפשר למנהלי מערכת להציג ולשנות את המצב של Drive Encryption (פעיל או לא פעיל), ולהציג את מצב ההצפנה של כל הכוננים הקשיחים במחשב.

- אם המצב לא פעיל, המאפיין Drive Encryption (הצפנת כונן) לא הופעל עדיין ב-HP ProtectTools Security Manager על-ידי מנהל המערכת של Windows והוא אינו מגן על הכונן הקשיח. השתמש באשף ההתקנה של HP ProtectTools Security Manager כדי להפעיל את Drive Encryption (הצפנת כונן).
- אם המצב פעיל, המאפיין Drive Encryption (הצפנת כונן) הופעל והוגדר. הכונן נמצא באחד מהמצבים הבאים:
  - Not encrypted (לא מוצפן)
  - Encrypted (מוצפן)
  - Encrypting (מצפין)
  - Decrypting (מפענח)

הצפנה או פענוח של כוננים בודדים

כדי להצפין כונן קשיח אחד או יותר במחשב או לפענח כונן שכבר הוצפן, השתמש במאפיין Change Encryption (שינוי הצפנה):

1. פתח את **HP ProtectTools Administrative Console**, לחץ על **Drive Encryption** (הצפנת כונן) ולאחר מכן לחץ על **Encryption Management** (ניהול הצפנה).
2. לחץ על **Change Encryption** (שינוי הצפנה).
3. בתיבת הדו-שיח Change Encryption (שינוי הצפנה), בחר או נקה את תיבת הסימון ליד כל כונן קשיח שברצונך להצפין או לפענח, ולאחר מכן לחץ על **OK** (אישור).

הערה: בעת ההצפנה או הפענוח של הכונן, סרגל התקדמות מציג את הזמן הנותר להשלמת התהליך במהלך ההפעלה הנוכחית. אם המחשב מכובה או נכנס למצב Sleep (שינה), Standby (המתנה), או Hibernation (מצב שינה) במהלך תהליך ההצפנה ולאחר מכן מופעל מחדש,תצוגת הזמן שנותר מתאפסת להתחלה, אך ההצפנה בפועל מתחדשת במקום שבו נקטעה לאחרונה. הזמן הנותר ותצוגת ההתקדמות ישתנו מהר יותר כדי לשקף את ההתקדמות הקודמת.

גיבוי ושחזור (משימה של מנהל מערכת)

הדף Recovery (שחזור) מאפשר למנהלי מערכת לגבות ולשחזר מפתחות הצפנה.

Local Drive Encryption Key Backup (גיבוי מפתח הצפנה של כונן מקומי)—האפשרות מאפשרת לך לגבות מפתחות הצפנה במדיה נשלפת בעת הפעלת Drive Encryption (הצפנת כונן).

יצירת מפתחות גיבוי

באפשרותך לגבות את מפתח ההצפנה של כונן מוצפן בהתקן אחסון נשלף:

זהירות: הקפד לשמור את התקן האחסון המכיל את מפתח הגיבוי במקום בטוח, משום שאם תשכח את הסיסמה או תאבד את כרטיס Java שלך, התקן זה יהווה את הגישה היחידה שלך לכונן הקשיח.

1. פתח את **HP ProtectTools Administrative Console**, לחץ על **Drive Encryption** (הצפנת כונן) ולאחר מכן לחץ על **Recovery** (שחזור).
2. לחץ על **Backup Keys** (מפתחות גיבוי).
3. בדף Select Backup Disk (בחירת דיסק לגיבוי), בחר את תיבת הסימון של ההתקן שבו ברצונך לגבות את מפתח ההצפנה ולאחר מכן לחץ על **Next** (הבא).
4. קרא את המידע בדף הבא שמוצג ולאחר מכן לחץ על **Next** (הבא). מפתח ההצפנה נשמר בהתקן האחסון שבחרת.
5. כאשר תיבת הדו-שיח לאישור נפתחת, לחץ על **Finish** (סיום).

ביצוע שחזור

כדי לבצע שחזור אם שכחת את הסיסמה, בצע את השלבים הבאים:

1. הפעל את המחשב.
2. הכנס את התקן האחסון הנשלף המכיל את מפתח הגיבוי.
3. בעת פתיחת תיבת הדו-שיח של הכניסה של Drive Encryption for HP ProtectTools, לחץ על **Cancel** (ביטול)
4. לחץ על **Options** (אפשרויות) בפינה השמאלית או הימנית התחתונה של המסך ולאחר מכן לחץ על **Recovery** (שחזור).
5. בחר את הקובץ שמכיל את מפתח הגיבוי או לחץ על **Browse** (עיון) כדי לחפש אחריו, ולאחר מכן לחץ על **Next** (הבא).
6. כאשר נפתחת תיבת הדו-שיח לאישור, לחץ על **OK** (אישור).

   המחשב מופעל.

הערה: מומלץ מאוד לאפס את הסיסמה לאחר ביצוע שחזור.

9 Privacy Manager for HP ProtectTools (בדגמים נבחרים בלבד)

Privacy Manager for HP ProtectTools מאפשר לך להשתמש בשיטות של כניסה מאובטחת מתקדמת (אימות) כדי לאמת את המקור, התקינות והאבטחה של תקשורת בעת השימוש בדואר אלקטרוני, מסמכי Microsoft® Office או הודעות מיידיות (IM).

Privacy Manager (מנהל הפרטיות) מנצל את תשתית האבטחה שמספק HP ProtectTools Security Manager, אשר כוללת את שיטות הכניסה המאובטחת הבאות:

- אימות טביעות אצבע
- סיסמת Windows®
- כרטיס HP ProtectTools Java™ Card

באפשרותך להשתמש בכל אחת משיטות הכניסה המאובטחת לעיל ב-Privacy Manager (מנהל הפרטיות).

Privacy Manager (מנהל הפרטיות) דורש את הפריטים הבאים:

- HP ProtectTools Security Manager 5.00 ואילך
- מערכת הפעלה Windows® 7, Windows Vista® או Windows XP
- Microsoft Outlook 2007 או Microsoft Outlook 2003
- חשבון דואר אלקטרוני חוקי

הערה: יש לבקש ולהתקין אישור של Privacy Manager (אישור דיגיטלי) מתוך Privacy Manager (מנהל הפרטיות) לפני שניתן יהיה לגשת למאפייני האבטחה. לקבלת מידע על בקשת אישור של Privacy Manager (מנהל הפרטיות), ראה בקשה והתקנה של אישור Privacy Manager (מנהל הפרטיות) בעמוד 44.

הליכי הגדרה

פתיחת Privacy Manager (מנהל הפרטיות)

כדי לפתוח את Privacy Manager (מנהל הפרטיות):

1. לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), לחץ על **HP** ולאחר מכן לחץ על **HP ProtectTools Security Manager**.
2. לחץ על **Privacy Manager** (מנהל הפרטיות).

- לחלופין -

לחץ לחיצה ימנית על הסמל של **HP ProtectTools** באזור ההודעות, בקצה הימני או השמאלי של שורת המשימות, לחץ על **Privacy Manager** (מנהל הפרטיות), ולאחר מכן לחץ על **Configuration** (תצורה).

- לחלופין -

בסרגל הכלים של הודעת דואר אלקטרוני של Microsoft Outlook, לחץ על החץ למטה ליד **Send Securely** (שליחה מאובטחת), ולאחר מכן לחץ על **Certificates** (אישורים) או **Trusted Contacts** (אנשי קשר מהימנים).

- לחלופין -

בסרגל הכלים של מסמך Microsoft Office, לחץ על החץ למטה ליד **Sign and Encrypt** (חתימה והצפנה), ולאחר מכן לחץ על **Certificates** (אישורים) או **Trusted Contacts** (אנשי קשר מהימנים).

ניהול אישורים של Privacy Manager (מנהל הפרטיות)

אישורים של Privacy Manager (מנהל הפרטיות) מגנים על נתונים והודעות באמצעות טכנולוגיית קריפטוגרפיה הנקראת תשתית מפתחות ציבורית (PKI). טכנולוגיית PKI דורשת ממשתמשים להשיג מפתחות קריפטוגרפיים ואישור של Privacy Manager (מנהל הפרטיות) מרשות אישורים (CA). בשונה מרוב תוכנות הצפנת הנתונים והאימות, אשר רק דורשות ממך לאמת את זהותך מדי פעם, Privacy Manager (מנהל הפרטיות) דורש אימות בכל פעם שאתה חותם על הודעת דואר אלקטרוני או מסמך של Microsft Office באמצעות מפתח קריפטוגרפי. Privacy Manager (מנהל הפרטיות) הופך את השמירה והשליחה של מידע חשוב לתהליך בטוח ומאובטח.

באפשרותך לבצע את המשימות הבאות:

- בקשה והתקנה של אישור Privacy Manager (מנהל הפרטיות)
- הצגת פרטי האישור של Privacy Manager (מנהל הפרטיות)
- חידוש אישורים של Privacy Manager (מנהל הפרטיות)
- כאשר קיימים אישורים מרובים, הגדרת אישור ברירת מחדל של Privacy Manager (מנהל הפרטיות) לשימוש בו
- מחיקה וביטול של אישור Privacy Manager (מנהל הפרטיות) (מתקדם)

בקשה והתקנה של אישור Privacy Manager (מנהל הפרטיות)

לפני שתוכל להשתמש במאפיינים של Privacy Manager (מנהל הפרטיות), עליך לבקש ולהתקין אישור של Privacy Manager (מתוך Privacy Manager) באמצעות כתובת דואר אלקטרוני חוקית. יש להגדיר את כתובת הדואר האלקטרוני בתור חשבון בתוך Microsoft Outlook באותו מחשב שממנו אתה מבקש את אישור Privacy Manager (מנהל הפרטיות).

בקשת אישור של Privacy Manager (מנהל הפרטיות)

1. פתח את Privacy Manager (מנהל הפרטיות) ולחץ על **Certificates** (אישורים).
2. לחץ על **Request a Privacy Manager certificate** (בקש אישור של מנהל הפרטיות).
3. בדף הפתיחה, קרא את הטקסט ולאחר מכן לחץ על **Next** (הבא).
4. בדף License Agreement (הסכם רשיון), קרא את הסכם הרשיון.
5. ודא שתיבת הסימון ליד **Check here to accept the terms of this license agreement** (סמן כאן כדי לקבל את התנאים של הסכם רשיון זה) נבחרה, ולאחר מכן לחץ על **Next** (הבא).
6. בדף Your Certificate Details (פרטי האישור שלך), הזן את המידע הדרוש ולאחר מכן לחץ על **Next** (הבא).
7. בדף Certificate Request Accepted (בקשה לאישור התקבלה), לחץ על **Finish** (סיום).
8. לחץ על **OK** (אישור) כדי לסגור את האישור.

ב-Microsoft Outlook, תקבל הודעת דואר אלקטרוני שלה יצורף האישור של Privacy Manager (מנהל הפרטיות).

השגת אישור חברה מוקצה מראש של Privacy Manager (מנהל הפרטיות)

1. ב-Outlook, פתח את הדואר האלקטרוני שקיבלת המציין שאישור חברה הוקצה מראש עבורך.
2. לחץ על **Obtain** (קבל).
3. ב-Microsoft Outlook, תקבל הודעת דואר אלקטרוני שלה יצורף האישור של Privacy Manager (מנהל הפרטיות).
4. כדי להתקין את האישור, ראה התקנת האישור של Privacy Manager (מנהל הפרטיות) בעמוד 45.

התקנת האישור של Privacy Manager (מנהל הפרטיות)

1. בעת קבלת הודעת הדואר האלקטרוני שלה מצורף אישור Privacy Manager (מנהל הפרטיות), פתח את ההודעה ולחץ על הלחצן **Setup** (התקן), בפינה הימנית או השמאלית התחתונה של ההודעה ב-Outlook 2007, או בפינה השמאלית או הימנית העליונה ב-Outlook 2003.
2. בצע אימות באמצעות שיטת הכניסה המאובטחת שבחרת.
3. בדף Certificate Installed (האישור הותקן), לחץ על **Next** (הבא).
4. בדף Certificate Backup (גיבוי אישור), הזן את המיקום והשם של קובץ הגיבוי או לחץ על **Browse** (עיון) לחיפוש המיקום.

△ **זהירות:** הקפד לשמור את הקובץ במיקום אחר פרט לכונן הקשיח ואחסן אותו במקום בטוח. קובץ זה נועד לשימושך בלבד, והוא דרוש למקרה שתצטרך לשחזר את אישור Privacy Manager (מנהל הפרטיות) והמפתחות המשויכים לו.

5. הזן ואשר את הסיסמה ולאחר מכן לחץ על **Next** (הבא).
6. בצע אימות באמצעות שיטת הכניסה המאובטחת שבחרת.
7. אם תבחר להתחיל את תהליך ההזמנה של איש קשר מהימן, פעל בהתאם להוראות על-גבי המסך החל משלב 2 של הנושא הוספת אנשי קשר מהימנים באמצעות אנשי קשר של Microsoft Outlook בעמוד 49.

   - לחלופין -

   אם תלחץ על **Cancel** (ביטול), ראה הוספת איש קשר מהימן בעמוד 48 לקבלת מידע על הוספת איש קשר מהימן בשלב מאוחר יותר.

הצגת פרטי האישור של Privacy Manager (מנהל הפרטיות)

1. פתח את Privacy Manager (מנהל הפרטיות) ולחץ על **Certificates** (אישורים).
2. לחץ על אישור של Privacy Manager (מנהל הפרטיות).
3. לחץ על **Certificate details** (פרטי אישור).
4. לאחר שסיימת להציג את הפרטים, לחץ על **OK** (אישור).

חידוש אישור של Privacy Manager (מנהל הפרטיות)

כאשר האישור של Privacy Manager (מנהל הפרטיות) עומד לפוג, תקבל הודעה שעליך לחדש אותו:

1. פתח את Privacy Manager (מנהל הפרטיות) ולחץ על **Certificates** (אישורים).
2. לחץ על **Renew certificate** (חדש אישור).
3. פעל בהתאם להוראות על-גבי המסך כדי לרכוש אישור חדש של Privacy Manager (מנהל הפרטיות).

הערה: תהליך החידוש של אישור Privacy Manager (מנהל הפרטיות) לא מחליף את האישור הישן של Privacy Manager שברשותך. יהיה עליך לרכוש אישור חדש של Privacy Manager (מנהל הפרטיות) ולהתקין אותו באמצעות אותם ההליכים כמו בנושא בקשה והתקנה של אישור Privacy Manager (מנהל הפרטיות) בעמוד 44.

הגדרת אישור ברירת מחדל של Privacy Manager (מנהל הפרטיות)

אישורי Privacy Manager (מנהל הפרטיות) הם האישורים הגלויים היחידים ב-Privacy Manager, גם אם מותקנים במחשב אישורים נוספים מרשויות אישורים אחרות.

אם קיים יותר מאישור אחד של Privacy Manager (מנהל הפרטיות) במחשב שהותקן מתוך Privacy Manager, באפשרותך לציין אישור אחד בתור ברירת המחדל:

1. פתח את Privacy Manager (מנהל הפרטיות) ולחץ על **Certificates** (אישורים).
2. לחץ על האישור של Privacy Manager (מנהל הפרטיות) שברצונך להשתמש בו כברירת המחדל, ולאחר מכן לחץ על **Set default** (הגדר כברירת מחדל).
3. לחץ על **OK** (אישור).

הערה: אינך נדרש להשתמש באישור ברירת המחדל של Privacy Manager (מנהל הפרטיות). מתוך הפונקציות השונות של Privacy Manager (מנהל הפרטיות), באפשרותך לבחור כל אישור של Privacy Manager לשימוש.

מחיקת אישור של Privacy Manager (מנהל הפרטיות)

אם תמחק אישור של Privacy Manager (מנהל הפרטיות), לא תוכל לפתוח קבצים כלשהם או להציג נתונים כלשהם שהצפנת באמצעות אישור זה. אם מחקת בטעות אישור של Privacy Manager (מנהל הפרטיות), תוכל לשחזר אותו באמצעות קובץ הגיבוי שיצרת בעת התקנת האישור. לקבלת מידע נוסף, עיין בסעיף שחזור אישור של Privacy Manager (מנהל הפרטיות) בעמוד 47.

כדי למחוק אישור של Privacy Manager (מנהל הפרטיות):

1. פתח את Privacy Manager (מנהל הפרטיות) ולחץ על **Certificates** (אישורים).
2. לחץ על האישור של Privacy Manager (מנהל הפרטיות) שברצונך למחוק ולאחר מכן לחץ על **Advanced** (מתקדם).
3. לחץ על **Delete** (מחק).

4. כאשר נפתחת תיבת הדו-שיח לאישור, לחץ על **Yes** (כן).

5. לחץ על **Close** (סגור) ולאחר מכן לחץ על **Apply** (החל).

שחזור אישור של Privacy Manager (מנהל הפרטיות)

במהלך ההתקנה של אישור Privacy Manager (מנהל הפרטיות), אתה נדרש ליצור עותק גיבוי של האישור. כמו כן, ייתכן שיצרת עותק גיבוי מדף ההעברה. ניתן להשתמש בעותק גיבוי זה בעת העברה למחשב אחר או לשחזור אישור באותו המחשב.

1. פתח את Privacy Manager (מנהל הפרטיות) ולחץ על **Migration** (העברה).

2. לחץ על **Restore** (שחזר).

3. בדף Migration File (קובץ העברה), לחץ על **Browse** (עיון) כדי לחפש את קובץ dppsm. שיצרת במהלך תהליך הגיבוי, ולאחר מכן לחץ על **Next** (הבא).

4. הזן את הסיסמה שבה השתמשת בעת יצירת הגיבוי ולאחר מכן לחץ על **Next** (הבא).

5. לחץ על **Finish** (סיום).

6. לחץ על **OK** (אישור).

ראה התקנת האישור של Privacy Manager (מנהל הפרטיות) בעמוד 45 או גיבוי אישורים ואנשי קשר מהימנים של Privacy Manager (מנהל הפרטיות) בעמוד 62 לקבלת מידע נוסף.

ביטול אישור של Privacy Manager (מנהל הפרטיות)

אם יש לך ספקות לגבי האבטחה של אישור Privacy Manager (מנהל הפרטיות) שברשותך, באפשרותך לבטל את האישור:

הערה: אישור Privacy Manager (מנהל הפרטיות) שבוטל לא נמחק. עדיין ניתן להשתמש באישור להצגת קבצים מוצפנים.

1. פתח את Privacy Manager (מנהל הפרטיות) ולחץ על **Certificates** (אישורים).

2. לחץ על **Advanced** (מתקדם).

3. לחץ על אישור Privacy Manager (מנהל הפרטיות) שברצונך לבטל ולאחר מכן לחץ על **Revoke** (ביטול).

4. כאשר נפתחת תיבת הדו-שיח לאישור, לחץ על **Yes** (כן).

5. בצע אימות באמצעות שיטת הכניסה המאובטחת שבחרת.

6. פעל לפי ההוראות שעל-גבי המסך.

ניהול אנשי קשר מהימנים

אנשי קשר מהימנים הם משתמשים שעימם החלפת אישורי Privacy Manager (מנהל הפרטיות), דבר המאפשר לכם לנהל תקשורת מאובטחת זה עם זה.

Trusted Contacts Manager (מנהל אנשי הקשר המהימנים) מאפשר לך לבצע את המשימות הבאות:

- הצגת פרטים של אנשי קשר מהימנים
- מחיקת אנשי קשר מהימנים
- בדיקת מצב ביטול של אנשי קשר מהימנים (מתקדם)

הוספת אנשי קשר מהימנים

הוספת אנשי קשר מהימנים היא תהליך בן 3 שלבים:

1. אתה שולח הזמנה בדואר אלקטרוני לנמען שברצונך להפוך לאיש קשר מהימן.
2. הנמען משיב לדואר האלקטרוני.
3. אתה מקבל את התגובה בדואר האלקטרוני מהנמען ולוחץ על **Accept** (קבל).

באפשרותך לשלוח הזמנות לאנשי קשר מהימנים בדואר האלקטרוני לנמענים בודדים או לכל אנשי הקשר בפנקס הכתובות של Microsoft Outlook.

עיין בסעיפים הבאים לשם הוספת אנשי קשר מהימנים.

הערה: כדי להשיב להזמנה שלך ולהפוך לאנשי קשר מהימנים, הנמענים חייבים להתקין את Privacy Manager (מנהל הפרטיות) במחשבים שברשותם או להתקין את הגרסה החלופית של הלקוח. לקבלת מידע נוסף אודות התקנה של לקוח חלופי, בקר באתר האינטרנט של DigitalPersona בכתובת http://DigitalPersona.com/PrivacyManager.

הוספת איש קשר מהימן

1. פתח את Privacy Manager (מנהל הפרטיות), לחץ על **Trusted Contacts Manager** (מנהל אנשי הקשר המהימנים), ולאחר מכן לחץ על **Invite Contacts** (הזמן אנשי קשר).

   - לחלופין -

   ב-Microsoft Outlook, לחץ על החץ למטה ליד **Send Securely** (שליחה מאובטחת) בסרגל הכלים ולאחר מכן לחץ על **Invite Contacts** (הזמן אנשי קשר).
2. אם תיבת הדו-שיח Select Certificate (בחירת אישור) נפתחת, לחץ על האישור של Privacy Manager (מנהל הפרטיות) שבו ברצונך להשתמש ולאחר מכן לחץ על **OK** (אישור).
3. כאשר נפתחת תיבת הדו-שיח Trusted Contact Invitation (הזמנת איש קשר מהימן), קרא את הטקסט ולאחר מכן לחץ על **OK** (אישור).

   הודעת דואר אלקטרוני נוצרת באופן אוטומטי.
4. הזן כתובת דואר אלקטרוני אחת או יותר של הנמענים שברצונך להוסיף בתור אנשי קשר מהימנים.
5. ערוך את הטקסט וחתום את שמך (אופציונלי).
6. לחץ על **Send** (שלח).

   הערה: אם לא השגת אישור של Privacy Manager (מנהל הפרטיות), מתקבלת הודעה שמוסרת לך כי עליך להשיג אישור זה כדי לשלוח בקשה של איש קשר מהימן. לחץ על **OK** (אישור) כדי להפעיל את Certificate Request Wizard (אשף בקשות האישורים). לקבלת מידע נוסף, עיין בסעיף בקשה והתקנה של אישור Privacy Manager (מנהל הפרטיות) בעמוד 44.
7. בצע אימות באמצעות שיטת הכניסה המאובטחת שבחרת.

   הערה: כאשר הנמען שברצונך להפוך לאיש קשר מהימן מקבל את הודעת הדואר האלקטרוני, עליו לפתוח אותה וללחוץ על **Accept** (קבל) בפינה הימנית או השמאלית התחתונה ולאחר מכן ללחוץ על **OK** (אישור) כשתיבת הדו-שיח לאישור מופיעה.
8. כאשר אתה מקבל תגובה בדואר אלקטרוני מנמען על כך שהוא מקבל את ההזמנה להפוך לאיש קשר מהימן, לחץ על **Accept** (קבל) בפינה הימנית או השמאלית התחתונה של הודעת הדואר האלקטרוני.

נפתחת תיבת דו-שיח המאשרת כי הנמען נוסף בהצלחה לרשימת אנשי הקשר המהימנים שלך.

9. לחץ על **OK** (אישור).

הוספת אנשי קשר מהימנים באמצעות אנשי קשר של Microsoft Outlook

1. פתח את Privacy Manager (מנהל הפרטיות), לחץ על **Trusted Contacts Manager** (מנהל אנשי הקשר המהימנים), ולאחר מכן לחץ על **Invite Contacts** (הזמן אנשי קשר).

   - לחלופין -

   ב-Microsoft Outlook, לחץ על החץ למטה ליד **Send Securely** (שליחה מאובטחת) בסרגל הכלים, ולאחר מכן לחץ על **Invite All My Outlook Contacts** (הזמן את כל אנשי הקשר שלי ב-Outlook).

2. כאשר הדף Trusted Contact Invitation (הזמנת איש קשר מאובטח) נפתח, בחר את כתובות הדואר האלקטרוני של הנמענים שברצונך להוסיף בתור אנשי קשר מהימנים ולאחר מכן לחץ על **Next** (הבא).

3. כאשר הדף Sending Invitation (שליחת הזמנה) נפתח, לחץ על **Finish** (סיום).

   הודעת דואר אלקטרוני המפרטת את כתובות הדואר האלקטרוני של Microsoft Outlook שנבחרו נוצרת באופן אוטומטי.

4. ערוך את הטקסט וחתום את שמך (אופציונלי).

5. לחץ על **Send** (שלח).

הערה: אם לא השגת אישור של Privacy Manager (מנהל הפרטיות), מתקבלת הודעה שמוסרת לך כי עליך להשיג אישור זה כדי לשלוח בקשה של איש קשר מהימן. לחץ על **OK** (אישור) כדי להפעיל את Certificate Request Wizard (אשף בקשות האישורים). לקבלת מידע נוסף, עיין בסעיף בקשה והתקנה של אישור Privacy Manager (מנהל הפרטיות) בעמוד 44.

6. בצע אימות באמצעות שיטת הכניסה המאובטחת שבחרת.

הערה: כאשר הנמען שברצונך להפוך לאיש קשר מהימן מקבל את הודעת הדואר האלקטרוני, עליו לפתוח אותה וללחוץ על **Accept** (קבל) בפינה הימנית או השמאלית התחתונה ולאחר מכן ללחוץ על **OK** (אישור) כשתיבת הדו-שיח לאישור מופיעה.

7. כאשר אתה מקבל תגובה בדואר אלקטרוני מנמען על כך שהוא מקבל את ההזמנה להפוך לאיש קשר מהימן, לחץ על **Accept** (קבל) בפינה הימנית או השמאלית התחתונה של הודעת הדואר האלקטרוני.

   נפתחת תיבת דו-שיח המאשרת כי הנמען נוסף בהצלחה לרשימת אנשי הקשר המהימנים שלך.

8. לחץ על **OK** (אישור).

הצגת פרטי איש קשר מהימן

1. פתח את Privacy Manager (מנהל הפרטיות) ולחץ על **Trusted Contacts** (אנשי קשר מהימנים).
2. לחץ על איש קשר מהימן.
3. לחץ על **Contact details** (פרטי איש קשר).
4. לאחר שסיימת להציג את הפרטים, לחץ על **OK** (אישור).

מחיקת איש קשר מהימן

1. פתח את Privacy Manager (מנהל הפרטיות) ולחץ על **Trusted Contacts** (אנשי קשר מהימנים).
2. לחץ על איש הקשר המהימן שברצונך למחוק.

3. לחץ על **Delete contact** (מחק איש קשר).
4. כאשר נפתחת תיבת הדו-שיח לאישור, לחץ על **Yes** (כן).

בדיקת מצב הביטול של איש קשר מהימן

כדי לראות את איש קשר מהימן ביטל את האישור שלו של Privacy Manager (מנהל הפרטיות):

1. פתח את Privacy Manager (מנהל הפרטיות) ולחץ על **Trusted Contacts** (אנשי קשר מהימנים).
2. לחץ על איש קשר מהימן.
3. לחץ על הלחצן **Advanced** (מתקדם).

   תיבת הדו-שיח Advanced Trusted Contact Management (ניהול מתקדם של אנשי קשר מהימנים) נפתחת.
4. לחץ על **Check Revocation** (בדוק ביטול).
5. לחץ על **Close** (סגור).

משימות כלליות

באפשרותך להשתמש ב-Privacy Manager (מנהל הפרטיות) עם מוצרי Microsoft הבאים:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

שימוש ב-Privacy Manager (מנהל הפרטיות) ב-Microsoft Outlook

בעת התקנת Privacy Manager (מנהל הפרטיות), לחצן Privacy (פרטיות) מוצג בסרגל הכלים של Microsoft Outlook, ולחצן Send Securely (שליחה מאובטחת) מוצג בסרגל הכלים של כל הודעת דואר אלקטרוני של Microsoft Outlook. בעת לחיצה על החץ למטה ליד **Privacy** (פרטיות) או **Send Securely** (שליחה מאובטחת), באפשרותך לבחור מהאפשרויות הבאות:

- Sign and Send (חתום ושלח) (לחצן Send Securely (שליחה מאובטחת) בלבד) - אפשרות זו מוסיפה חתימה דיגיטלית לדואר האלקטרוני ושולחת אותו לאחר האימות באמצעות שיטת הכניסה המאובטחת שבחרת.
- Seal for Trusted Contacts and Send (הוסף חותם עבור אנשי קשר מהימנים ושלח) (לחצן Send Securely (שליחה מאובטחת) בלבד) - אפשרות זו מוסיפה חתימה דיגיטלית, מצפינה את הדואר האלקטרוני ושולחת אותו לאחר האימות באמצעות שיטת הכניסה המאובטחת שבחרת.
- Invite Contacts (הזמן אנשי קשר) - אפשרות זו מאפשרת לך לשלוח הזמנה לאיש קשר מאובטח. לקבלת מידע נוסף, עיין בסעיף הוספת איש קשר מהימן בעמוד 48.
- Invite Outlook Contacts (הזמן אנשי קשר של Outlook) - אפשרות זו מאפשרת לך לשלוח הזמנה לאיש קשר מהימן לכל אנשי הקשר בפנקס הכתובות של Microsoft Outlook. לקבלת מידע נוסף, עיין בסעיף הוספת אנשי קשר מהימנים באמצעות אנשי קשר של Microsoft Outlook בעמוד 49.
- Open the Privacy Manager software (פתח את תוכנת מנהל הפרטיות) - אפשרויות של אישורים, אנשי קשר מהימנים והגדרות מאפשרות לך לפתוח את תוכנת Privacy Manager (מנהל הפרטיות) כדי להוסיף, להציג או לשנות את ההגדרות הנוכחיות. לקבלת מידע נוסף, עיין בסעיף הגדרת התצורה של Privacy Manager (מנהל הפרטיות) עבור Microsoft Outlook בעמוד 51.

הגדרת התצורה של Privacy Manager (מנהל הפרטיות) עבור Microsoft Outlook

1. פתח את Privacy Manager (מנהל הפרטיות), לחץ על **Settings** (הגדרות) ולאחר מכן לחץ על הכרטיסייה **E-mail** (דואר אלקטרוני).

   - לחלופין -

   בסרגל הכלים הראשי של Microsoft Outlook, לחץ על החץ למטה ליד **Send Securely** (שליחה מאובטחת) (**Privacy** (פרטיות) ב-Outlook 2003), ולאחר מכן לחץ על **Settings** (הגדרות).

   - לחלופין -

   בסרגל הכלים של הודעת דואר אלקטרוני של Microsoft, לחץ על החץ למטה ליד **Send Securely** (שליחה מאובטחת), ולאחר מכן לחץ על **Settings** (הגדרות).
2. בחר את הפעולות שברצונך לבצע בעת שליחת דואר אלקטרוני מאובטח ולאחר מכן לחץ על **OK** (אישור).

חתימה ושליחה של הודעת דואר אלקטרוני

1. ב-Microsoft Outlook, לחץ על **New** (חדש) או **Reply** (השב).
2. הקלד את הודעת הדואר האלקטרוני.

3. לחץ על החץ למטה ליד **Send Securely** (שליחה מאובטחת) **Privacy** (פרטיות) ב-Outlook 2003), ולאחר מכן לחץ על **Sign and Send** (חתום ושלח).

4. בצע אימות באמצעות שיטת הכניסה המאובטחת שבחרת.

הוספת חותם ושליחה של הודעת דואר אלקטרוני

רק אנשים שבחרת מרשימת אנשי הקשר המהימנים יכולים להציג הודעות דואר אלקטרוני עם חותם אשר נחתמו דיגיטלית ונוסף להן חותם (הוצפנו).

כדי להוסיף חותם ולשלוח הודעת דואר אלקטרוני לאיש קשר מהימן:

1. ב-Microsoft Outlook, לחץ על **New** (חדש) או **Reply** (השב).

2. הקלד את הודעת הדואר האלקטרוני.

3. לחץ על החץ למטה ליד **Send Securely** (שליחה מאובטחת) **Privacy** (פרטיות) ב-Outlook 2003), ולאחר מכן לחץ על **Seal for Trusted Contacts and Send** (הוסף חותם עבור אנשי קשר מהימנים ושלח).

4. בצע אימות באמצעות שיטת הכניסה המאובטחת שבחרת.

הצגת הודעת דואר אלקטרוני עם חותם

בעת פתיחת הודעת דואר אלקטרוני עם חותם, תווית האבטחה מוצגת בכותרת של הדואר האלקטרוני. תווית האבטחה מספקת את המידע הבא:

- אילו אישורים שימשו לאימות זהות האדם שחתם על הדואר האלקטרוני
- המוצר ששימש לאימות האישורים של האדם שחתם על הדואר האלקטרוני

שימוש ב-Privacy Manager (מנהל הפרטיות) במסמך של Microsoft Office 2007

הערה: ניתן להשתמש ב-Privacy Manager (מנהל הפרטיות) עם מסמכי Microsoft Office 2007 בלבד.

לאחר ההתקנה של אישור של Privacy Manager (מנהל הפרטיות), לחצן Sign and Encrypt (חתימה והצפנה) מוצג בצד הימני או השמאלי של סרגל הכלים של כל מסמכי Microsoft Word, Microsoft Excel ו-Microsoft PowerPoint. בעת לחיצה על החץ למטה ליד **Sign and Encrypt** (חתימה והצפנה), באפשרותך לבחור מבין האפשרויות הבאות:

- Sign Document (חתום על מסמך) - אפשרות זו מוסיפה את החתימה הדיגיטלית שלך למסמך.
- Add Signature Line Before Signing (הוסף שורת חתימה לפני החתימה) (Microsoft Word ו-Microsoft Excel בלבד) - כברירת מחדל, שורת חתימה נוספת בעת חתימה והצפנה של מסמך Microsoft Word או Microsoft Excel. כדי לבטל אפשרות זו, לחץ על **Add Signature Line** (הוסף שורת חתימה) כדי להסיר את סימן הביקורת.
- Encrypt Document (הצפן מסמך) - אפשרות זו מוסיפה את החתימה הדיגיטלית שלך ומצפינה את המסמך.
- Remove Encryption (הסר הצפנה) - אפשרות זו מסירה את ההצפנה מהמסמך.
- Open the Privacy Manager software (פתח את תוכנת מנהל הפרטיות) - אפשרויות של אישורים, אנשי קשר מהימנים והגדרות מאפשרות לך לפתוח את תוכנת Privacy Manager (מנהל הפרטיות) כדי להוסיף, להציג או לשנות את ההגדרות הנוכחיות. ראה ניהול אישורים של Privacy Manager (מנהל הפרטיות) בעמוד 44, ניהול אנשי קשר מהימנים בעמוד 47, או הגדרת התצורה של Privacy Manager (מנהל הפרטיות) עבור Microsoft Office בעמוד 53 לקבלת מידע נוסף.

הגדרת התצורה של Privacy Manager (מנהל הפרטיות) עבור Microsoft Office

1. פתח את Privacy Manager (מנהל הפרטיות), לחץ על **Settings** (הגדרות) ולאחר מכן לחץ על הכרטיסייה **Documents** (מסמכים).

   - לחלופין -

   בסרגל הכלים של מסמך Microsoft Office, לחץ על החץ למטה ליד **Sign and Encrypt** (חתימה והצפנה) ולאחר מכן לחץ על **Settings** (הגדרות).

2. בחר את הפעולות שברצונך להגדיר את תצורתן ולאחר מכן לחץ על **OK** (אישור).

חתימה על מסמך Microsoft Office

1. ב-Microsoft Word, ‏Microsoft Excel או Microsoft PowerPoint, צור ושמור מסמך.
2. לחץ על החץ למטה ליד **Sign and Encrypt** (חתימה והצפנה) ולאחר מכן לחץ על **Sign Document** (חתום על מסמך).
3. בצע אימות באמצעות שיטת הכניסה המאובטחת שבחרת.
4. כאשר מופיעה תיבת הדו-שיח לאישור, קרא את הטקסט ולאחר מכן לחץ על **OK** (אישור).

אם תחליט בשלב מאוחר יותר לערוך את המסמך, בצע את השלבים הבאים:

1. לחץ על לחצן **Office** בפינה השמאלית או הימנית העליונה של המסך.
2. לחץ על **Prepare** (הכן) ולאחר מכן לחץ על **Mark as Final** (סמן כסופי).
3. כאשר תיבת הדו-שיח לאישור נפתחת, לחץ על **Yes** (כן) והמשך לעבוד.
4. לאחר שתשלים את העריכה, חתום שוב על המסמך.

הוספת שורת חתימה בעת חתימה על מסמך Microsoft Word או Microsoft Excel

Privacy Manager (מנהל הפרטיות) מאפשר לך להוסיף שורת חתימה בעת חתימה על מסמך Microsoft Word או Microsoft Excel:

1. ב-Microsoft Word או Microsoft Excel, צור ושמור מסמך.
2. לחץ על תפריט **Home** (בית).
3. לחץ על החץ למטה ליד **Sign and Encrypt** (חתימה והצפנה), ולאחר מכן לחץ על **Add Signature Line Before Signing** (הוסף שורת חתימה לפני החתימה).

   הערה: סימן ביקורת מוצג ליד האפשרות Add Signature Line Before Signing (הוסף שורת חתימה לפני החתימה) כאשר אפשרות זו נבחרת. כברירת מחדל, אפשרות זו פועלת.

4. לחץ על החץ למטה ליד **Sign and Encrypt** (חתימה והצפנה) ולאחר מכן לחץ על **Sign Document** (חתום על מסמך).
5. בצע אימות באמצעות שיטת הכניסה המאובטחת שבחרת.

הוספת חותמים מוצעים למסמך Microsoft Word או Microsoft Excel

באפשרותך להוסיף יותר משורת חתימה אחת למסמך על-ידי ציון חותמים מוצעים. חותם מוצע הוא משתמש שהבעלים של מסמך Microsoft Word או Microsoft Excel מייעד להוספת שורת חתימה למסמך. אתה יכול לשמש כחותם מוצע, או אדם אחר שברצונך שיחתום על המסמך שלך. לדוגמה, אם אתה מכין מסמך שדורש חתימה של כל חברי המחלקה,

באפשרותך לכלול שורות חתימה עבור משתמשים אלה בתחתית העמוד האחרון של המסמך, עם הוראות לחתימה עד לתאריך ספציפי.

כדי להוסיף חותם מוצע למסמך Microsoft Word או Microsoft Excel:

1. ב-Microsoft Word או Microsoft Excel, צור ושמור מסמך.
2. לחץ על תפריט **Insert** (הוספה).
3. בקבוצה **Text** (טקסט) בסרגל הכלים, לחץ על החץ ליד **Signature Line** (שורת חתימה) ולאחר מכן לחץ על **Privacy Manager Signature Provider** (ספק חתימה של מנהל הפרטיות).

   תיבת הדו-שיח Signature Setup (הגדרת חתימה) נפתחת.
4. בתיבת הטקסט תחת **Suggested signer** (חותם מוצע), הזן את שמו של החותם המוצע.
5. בתיבת הטקסט תחת **Instructions to the signer** (הוראות לחותם), הזן הודעה עבור חותם מוצע זה.

הערה: הודעה זו תופיע במקום תפקיד, והיא תימחק או תוחלף על-ידי תפקיד המשתמש בעת חתימת המסמך.

6. בחר את תיבת הסימון **Show sign date in signature line** (הצג תאריך חתימה בשורת החתימה) כדי להציג את התאריך.
7. בחר את תיבת הסימון **Show signer's title in signature line** (הצג תפקיד חותם בשורת החתימה) כדי להציג את התפקיד.

הערה: מכיוון שהבעלים של המסמך מקצה חותמים מוצעים למסמך שלו, אם תיבות הסימון **Show sign date in signature line** (הצג תאריך חתימה בשורת החתימה) ו/או **Show signer's title in signature line** (הצג תפקיד חותם בשורת החתימה) אינן מסומנות, החותם המוצע לא יוכל להציג את התאריך ו/או את התפקיד בשורת החתימה גם אם הגדרות המסמך של החותם המוצע מוגדרות לבצע זאת.

8. לחץ על **OK** (אישור).

הוספת שורת חתימה של חותם מוצע

כאשר חותמים מוצעים פותחים את המסמך, הם רואים את שמם בסוגריים מרובעים כדי לציין שחתימתם דרושה.

כדי לחתום על המסמך:

1. לחץ לחיצה כפולה על שורת החתימה המתאימה.
2. בצע אימות באמצעות שיטת הכניסה המאובטחת שבחרת.

   שורת החתימה תוצג בהתאם להגדרות שצוינו על-ידי הבעלים של המסמך.

הצפנת מסמך Microsoft Office

באפשרותך להצפין מסמך Microsoft Office עבורך ועבור אנשי הקשר המהימנים שלך. כאשר מסמך מוצפן ונסגר, אתה ואנשי הקשר מהימנים שבחרת מהרשימה חייבים לבצע אימות לפני פתיחתו.

כדי להצפין מסמך Microsoft Office:

1. ב-Microsoft Word, Microsoft Excel או Microsoft PowerPoint, צור ושמור מסמך.
2. לחץ על תפריט **Home** (בית).
3. לחץ על החץ למטה ליד **Sign and Encrypt** (חתימה והצפנה) ולאחר מכן לחץ על **Encrypt Document** (הצפן מסמך).

   תיבת הדו-שיח Select Trusted Contacts (בחירת אנשי קשר מהימנים) נפתחת.

4. לחץ על שמו של איש קשר מהימן שיוכל לפתוח את המסמך ולהציג את תוכנו.

הערה: כדי לבחור שמות מרובים של אנשי קשר מהימנים, החזק את מקש ctrl לחוץ ולחץ על השמות הנפרדים.

5. לחץ על **OK** (אישור).

אם תחליט בשלב מאוחר יותר לערוך את המסמך, בצע את השלבים בנושא הסרת הצפנה ממסמך Microsoft Office בעמוד 55. לאחר הסרת ההצפנה, תוכל לערוך את המסמך. בצע את השלבים בסעיף זה כדי להצפין שוב את המסמך.

הסרת הצפנה ממסמך Microsoft Office

בעת הסרת הצפנה ממסמך Microsoft Office, אתה ואנשי הקשר המהימנים לא נדרשים עוד לבצע אימות כדי לפתוח ולהציג את תוכן המסמך.

כדי להסיר הצפנה ממסמך Microsoft Office:

1. פתח מסמך מוצפן של Microsoft Word ,Microsoft Excel או Microsoft PowerPoint.
2. בצע אימות באמצעות שיטת הכניסה המאובטחת שבחרת.
3. לחץ על תפריט **Home** (בית).
4. לחץ על החץ למטה ליד **Sign and Encrypt** (חתימה והצפנה) ולאחר מכן לחץ על **Remove Encryption** (הסר הצפנה).

שליחת מסמך מוצפן של Microsoft Office

באפשרותך לצרף מסמך מוצפן של Microsoft Office להודעת דואר אלקטרוני מבלי לחתום או להצפין את ההודעה עצמה. לשם כך, צור ושלח דואר אלקטרוני עם מסמך חתום או מצופן כפי שהיית עושה עם דואר אלקטרוני רגיל עם מסמך מצורף.

עם זאת, לקבלת אבטחה מרבית, מומלץ להצפין את הדואר האלקטרוני בעת צירוף מסמך חתום או מוצפן של Microsoft Office.

כדי לשלוח דואר אלקטרוני עם חותם ומסמך חתום ו/או מוצפן של Microsoft Office, בצע את השלבים הבאים:

1. ב-Microsoft Outlook, לחץ על **New** (חדש) או **Reply** (השב).
2. הקלד את הודעת הדואר האלקטרוני.
3. צרף את המסמך של Microsoft Office.
4. עיין בנושא הוספת חותם ושליחה של הודעת דואר אלקטרוני בעמוד 52 לקבלת הוראות נוספות.

הצגת מסמך חתום של Microsoft Office

הערה: אינך זקוק לאישור של Privacy Manager (מנהל הפרטיות) כדי להציג מסמך חתום של Microsoft Office.

בעת פתיחה של מסמך חתום של Microsoft Office, סמל חתימה דיגיטלית מוצג בשורת המצב בתחתית חלון המסמך.

1. לחץ על סמל **Digital Signatures** (חתימות דיגיטליות) כדי להציג או לבטל את ההצגה של תיבת הדו-שיח Signatures (חתימות), אשר מציגה את שמות כל המשתמשים שחתמו על המסמך והתאריכים של כל החתימות.
2. כדי להציג פרטים נוספים על כל חתימה, לחץ לחיצה ימנית על שם בתיבת הדו-שיח Signatures (חתימות) ובחר Signature Details (פרטי חתימה).

הצגת מסמך מוצפן של Microsoft Office

כדי להציג מסמך מוצפן של Microsoft Office ממחשב אחר, Privacy Manager (מנהל הפרטיות) חייב להיות מותקן באותו מחשב. בנוסף, עליך לשחזר את אישור Privacy Manager (מנהל הפרטיות) ששימש להצפנת הקובץ.

איש קשר מהימן המעוניין להציג מסמך מוצפן של Microsoft Office זקוק לאישור של Privacy Manager (מנהל הפרטיות), ותוכנה זו חייבת להיות מותקנת במחשבו. בנוסף, הבעלים של המסמך המוצפן של Microsoft Office חייב לבחור את איש הקשר המהימן.

שימוש ב-Privacy Manager (מנהל הפרטיות) ב-Windows Live Messenger

Privacy Manager (מנהל הפרטיות) מוסיף את מאפייני התקשורת המאובטחת הבאים ל-Windows Live Messenger:

- **Secure chat** (צ'אט מאובטח) - הודעות משודרות באמצעות פרוטוקול SSL/TLS (Secure Sockets Layer/Transport Layer Security) באמצעות XML, אותה טכנולוגיה המאבטחת עסקאות מסחר אלקטרוני.
- **Recipient identification** (זיהוי נמען) - באפשרותך לאמת את הנוכחות והזהות של אדם כלשהו לפני שליחת הודעה.
- **Signed messages** (הודעות חתומות) - באפשרותך לחתום על ההודעות שלך באופן אלקטרוני. לאחר מכן, אם נעשה שימוש לרעה בהודעה, היא תסומן כלא חוקית כאשר הנמען יקבל אותה.
- **Hide/show feature** (מאפיין הסתרה/הצגה) - באפשרותך להסתיר הודעה כלשהי או את כל ההודעות בחלון הצ'אט של Privacy Manager (מנהל הפרטיות). כמו כן, באפשרותך לשלוח הודעה שהתוכן שבה מוסתר. לשם הצגת ההודעה, יש לבצע אימות.
- **Secure chat history** (היסטוריית צ'אטים מאובטחים) - יומני הפעלות צ'אט מוצפנים לפני שמירתם והם דורשים אימות לשם הצגה.
- **Automatic locking/unlocking** (נעילה/ביטול נעילה אוטומטיים) - באפשרותך לנעול ולבטל את הנעילה של חלון הצ'אט של Privacy Manager (מנהל הפרטיות) או להגדיר נעילה אוטומטית של החלון לאחר פרק זמן שצוין של חוסר פעילות.

התחלת הפעלת צ'אט של Privacy Manager (מנהל הפרטיות)

הערה: כדי להשתמש בצ'אט של Privacy Manager (מנהל הפרטיות), על שני הצדדים להתקין את Privacy Manager ואישור של Privacy Manager. לקבלת פרטים אודות התקנת אישור של Privacy Manager (מנהל הפרטיות), ראה בקשה והתקנה של אישור Privacy Manager (מנהל הפרטיות) בעמוד 44.

1. כדי להתחיל בצ'אט של Privacy Manager (מנהל הפרטיות) ב-Windows Live Messenger, בצע אחד מההליכים הבאים:

   א. לחץ לחיצה ימנית על איש קשר מקוון ב-Live Messenger, ולאחר מכן בחר **Start an Activity** (התחל פעילות).

   ב. לחץ על **Start Chat** (התחל צ'אט).

   - לחלופין -

   א. לחץ לחיצה כפולה על איש קשר מקוון ב-Live Messenger ולאחר מכן בחר את תפריט **See a list of activities** (ראה רשימת פעילויות).

   ב. לחץ על **Action** (פעולה) ולאחר מכן לחץ על **Start Chat** (התחל צ'אט).

- לחלופין -

א. לחץ לחיצה ימנית על סמל **ProtectTools** באזור ההודעות, לחץ על **Privacy Manager for HP ProtectTools**, ולאחר מכן בחר **Start Chat** (התחל צ'אט).

ב. ב-Live Messenger, לחץ על **Actions: Start an Activity** (פעולות: התחל פעילות), ולאחר מכן בחר **Privacy Manager Chat** (צ'אט של מנהל הפרטיות).

הערה: כל משתמש חייב להיות מקוון ב-Live Messenger והמשתמשים חייבים להיות מוצגים זה אצל זה בחלון המקוון של Live Messenger. לחץ כדי לבחור משתמש מקוון.

Privacy Manager (מנהל הפרטיות) שולח הזמנה לאיש הקשר כדי להתחיל צ'אט של Privacy Manager. כאשר איש הקשר המוזמן מקבל את ההזמנה, חלון הצ'אט של Privacy Manager (מנהל הפרטיות) נפתח. אם Privacy Manager (מנהל הפרטיות) אינו מותקן אצל איש הקשר המוזמן, תוצג לו בקשה להוריד את התוכנה.

2. לחץ על **Start** (התחל) כדי להתחיל בצ'אט המאובטח.

הגדרת התצורה של Privacy Manager (מנהל הפרטיות) עבור Windows Live Messenger

1. בצ'אט של Privacy Manager (מנהל הפרטיות), לחץ על הלחצן **Settings** (הגדרות).

- לחלופין -

ב-Privacy Manager (מנהל הפרטיות), לחץ על **Settings** (הגדרות) ולאחר מכן לחץ על הכרטיסייה **Chat** (צ'אט).

- לחלופין -

ב-Live Messenger History Viewer של Privacy Manager (מנהל הפרטיות), לחץ על הלחצן **Settings** (הגדרות).

2. כדי לציין את פרק הזמן שהצ'אט של Privacy Manager (מנהל הפרטיות) ממתין לפני נעילת ההפעלה, בחר מספר מהרשימה **Lock session after _ minutes of activity** (נעל הפעלה לאחר _ דקות של חוסר פעילות).

3. כדי לציין תיקיית היסטוריה עבור הפעלות הצ'אט, לחץ על **Browse** (עיון) כדי לחפש תיקייה ולאחר מכן לחץ על **OK** (אישור).

4. כדי להצפין ולשמור את ההפעלות באופן אוטומטי בעת סגירתן, בחר את תיבת הסימון **Automatically save secure chat history** (שמור היסטוריית צ'אטים מאובטחים באופן אוטומטי).

5. לחץ על **OK** (אישור).

ניהול צ'אטים בחלון הצ'אט של Privacy Manager (מנהל הפרטיות)

לאחר הפעלת צ'אט של Privacy Manager (מנהל הפרטיות), חלון צ'אט של Privacy Manager נפתח ב-Windows Live Messenger. השימוש בצ'אט של Privacy Manager (מנהל הפרטיות) דומה לשימוש הבסיסי ב-Windows Live Messenger, פרט לכך שהמאפיינים הבאים זמינים בחלון הצ'אט של Privacy Manager:

- **Save** (שמור) - לחץ על לחצן זה כדי לשמור את הפעלת הצ'אט בתיקייה שציינת בהגדרות התצורה. כמו כן, באפשרותך להגדיר את הצ'אט של Privacy Manager (מנהל הפרטיות) לשמור באופן אוטומטי כל הפעלה כאשר היא נסגרת.
- **Hide all** (הסתר הכל) ו-**Show all** (הצג הכל) - לחץ על הלחצן המתאים כדי להרחיב או לכווץ את ההודעות המוצגות בחלון Secure Communications (תקשורת מאובטחת). כמו כן, באפשרותך להסתיר או להציג הודעות נפרדות על-ידי לחיצה על כותרת ההודעה.
- **?Are you there** (אתה נמצא?) - לחץ על לחצן זה כדי לבקש אימות מאיש הקשר.

- **Lock** (נעל) - לחץ על לחצן זה כדי לסגור את חלון הצ'אט של Privacy Manager (מנהל הפרטיות) ולחזור לחלון Chat Entry (כניסה לצ'אט). כדי להציג שוב את החלון Secure Communications (תקשורת מאובטחת), לחץ על **Resume the session** (חדש את ההפעלה), ולאחר מכן בצע אימות באמצעות שיטת הכניסה המאובטחת הנבחרת שלך.
- **Send** (שלח) - לחץ על לחצן זה כדי לשלוח הודעה מוצפנת לאיש הקשר.
- **Send signed** (שלח עם חתימה) - בחר תיבת סימון זו כדי לחתום באופן אלקטרוני ולהצפין את ההודעות. לאחר מכן, אם נעשה שימוש לרעה בהודעה, היא תסומן כלא חוקית כאשר הנמען יקבל אותה. עליך לבצע אימות בכל פעם שאתה שולח הודעה חתומה.
- **Send hidden** (שלח מוסתר) - בחר תיבת סימון זו כדי להצפין ולשלוח הודעה המציגה כותרת בלבד. איש הקשר יצטרך לבצע אימות כדי לקרוא את תוכן ההודעה.

הצגת היסטוריית צ'אטים

הצ'אט של Privacy Manager (מנהל הפרטיות): Live Messenger History Viewer מציג קובצי הפעלה מוצפנים של הצ'טים של Privacy Manager. ניתן לשמור הפעלות על-ידי לחיצה על **Save** (שמור) בחלון הצ'אט של Privacy Manager (מנהל הפרטיות), או על-ידי הגדרת שמירה אוטומטית בכרטיסייה Chat (צ'אט) ב-Privacy Manager. במציג, כל הפעלה מציגה את הגרסה המוצפנת של שם המסך של איש הקשר, ואת התאריך והשעה שבהם ההפעלה התחילה והסתיימה. כברירת מחדל, הפעלות מוצגות עבור כל חשבונות הדואר האלקטרוני שהגדרת. באפשרותך להשתמש בתפריט **Display history for** (הצג היסטוריה עבור) כדי לבחור בהצגה של חשבונות ספציפיים בלבד.

המציג מאפשר לך לבצע את המשימות הבאות:

- חשיפת כל ההפעלות בעמוד 58
- חשיפת הפעלות של חשבון ספציפי בעמוד 59
- הצגת מזהה הפעלה בעמוד 59
- הצגת הפעלה בעמוד 59
- חיפוש טקסט ספציפי בהפעלות בעמוד 59
- מחיקת הפעלה בעמוד 60
- הוספה או הסרה של עמודות בעמוד 60
- סינון הפעלות מוצגות בעמוד 60

כדי להפעיל את Live Messenger History Viewer:

▲ באזור ההודעות, בקצה הימני או השמאלי של שורת המשימות, לחץ לחיצה ימנית על סמל **HP ProtectTools**, לחץ על **Privacy Manager: for HP ProtectTools**, ולאחר מכן לחץ על **Live Messenger History Viewer**.

- לחלופין -

▲ בהפעלת צ'אט, לחץ על **History Viewer** (מציג ההיסטוריה) או **History** (היסטוריה).

חשיפת כל ההפעלות

חשיפת כל ההפעלות מציגה את שם המסך המוצפן של איש הקשר של ההפעלות הנוכחיות שנבחרו וכל ההפעלות באותו החשבון.

כדי לחשוף את כל הפעלות הצ'אט השמורות בהיסטוריה:

1. ב-Live Messenger History Viewer, לחץ לחיצה ימנית על הפעלה כלשהי ולאחר מכן בחר **Reveal All Sessions** (חשוף את כל ההפעלות).
2. בצע אימות באמצעות שיטת הכניסה המאובטחת שבחרת.

   שמות המסך של אנשי הקשר מוצפנים.
3. לחץ לחיצה כפולה על הפעלה כלשהי כדי להציג את תוכנה.

חשיפת הפעלות של חשבון ספציפי

חשיפת הפעלה מציגה את שם המסך המוצפן של איש הקשר של ההפעלה הנוכחית שנבחרה.

כדי לחשוף הפעלת צ'אט ספציפית בהיסטוריה:

1. ב-Live Messenger History Viewer, לחץ לחיצה ימנית על הפעלה כלשהי ולאחר מכן בחר **Reveal Session** (חשוף הפעלה).
2. בצע אימות באמצעות שיטת הכניסה המאובטחת שבחרת.

   שם המסך של איש הקשר מפוענח.
3. לחץ לחיצה כפולה על הפעלה חשופה כדי להציג את תוכנה.

הערה: הפעלות נוספות שהוצפנו באמצעות אותו האישור יציגו סמל של ביטול נעילה, המציין שבאפשרותך להציג אותן על-ידי לחיצה כפולה עליהן ללא אימות נוסף. הפעלות המוצפנות באמצעות אישור אחר יציגו סמל נעול, המציין שדרוש אימות נוסף עבור הפעלות אלה לפני שניתן יהיה להציג את שמות המסך של אנשי הקשר או התוכן.

הצגת מזהה הפעלה

כדי להציג מזהה הפעלה:

▲ ב-Live Messenger History Viewer, לחץ לחיצה ימנית על הפעלה חשופה כלשהי ובחר **View session ID** (הצג מזהה הפעלה).

הצגת הפעלה

הצגת הפעלה פותחת את הקובץ להצגה. אם ההפעלה לא נחשפה עדיין (מוצגת עם שם מסך מוצפן של איש קשר), היא נחשפת באותו הזמן.

כדי להציג הפעלה בהיסטוריה של Live Messenger:

1. ב-Live Messenger History Viewer, לחץ לחיצה ימנית על הפעלה כלשהי ולאחר מכן בחר **View** (הצג).
2. אם תתבקש, בצע אימות באמצעות שיטת הכניסה המאובטחת שבחרת.

   תוכן ההפעלה מפוענח.

חיפוש טקסט ספציפי בהפעלות

ניתן לבצע חיפוש טקסט רק בהפעלות חשופות (מפוענחות) המוצגות בחלון המציג. אלה הן ההפעלות שבהן שם המסך של איש הקשר מוצג בטקסט רגיל.

כדי לחפש טקסט בהפעלות צ'אט בהיסטוריה:

1. ב-Live Messenger History Viewer, לחץ על הלחצן **Search** (חיפוש).
2. הזן את הטקסט לחיפוש, הגדר פרמטרי חיפוש רצויים ולאחר מכן לחץ על **OK** (אישור).

הפעלות המכילות את הטקסט מודגשות בחלון המציג.

מחיקת הפעלה

1. בחר הפעלת צ'אט בהיסטוריה.
2. לחץ על **Delete** (מחק).

הוספה או הסרה של עמודות

כברירת מחדל, 3 העמודות הנמצאות בשימוש הרב ביותר מוצגות ב-Live Messenger History Viewer. באפשרותך להוסיף עמודות נוספות לתצוגה או להסיר עמודות ממנה.

כדי להוסיף עמודות לתצוגה:

1. לחץ לחיצה ימנית על כותרת עמודה כלשהי ולאחר מכן בחר **Add/Remove Columns** (הוסף/הסר עמודות).
2. בחר כותרת עמודה בלוח השמאלי או הימני ולאחר מכן לחץ על **Add** (הוסף) כדי להעביר אותה ללוח הנגדי.

כדי להסיר עמודות מהתצוגה:

1. לחץ לחיצה ימנית על כותרת עמודה כלשהי ולאחר מכן בחר **Add/Remove Columns** (הוסף/הסר עמודות).
2. בחר כותרת עמודה בלוח הימני או השמאלי ולאחר מכן לחץ על **Remove** (הסר) כדי להעביר אותה ללוח הנגדי.

סינון הפעלות מוצגות

רשימת הפעלות של כל החשבונות מוצגת ב-Live Messenger History Viewer. באפשרותך גם לסנן את ההפעלות המוצגות לפי הפריטים הבאים:

- חשבונות ספציפיים. לקבלת פרטים, ראה הצגת הפעלות של חשבון ספציפי בעמוד 60.
- טווח תאריכים. לקבלת פרטים, ראה הצגת הפעלות לפי טווח תאריכים בעמוד 60.
- תיקיות שונות. לקבלת פרטים, ראה הצגת הפעלות שנשמרו בתיקייה שאינה תיקיית ברירת המחדל בעמוד 60.

הצגת הפעלות של חשבון ספציפי

▲ ב-Live Messenger History Viewer, בחר חשבון מתוך תפריט **Display history for** (הצג היסטוריה עבור).

הצגת הפעלות לפי טווח תאריכים

1. ב-Live Messenger History Viewer, לחץ על סמל **Advanced Filter** (סינון מתקדם).

   תיבת הדו-שיח Advanced Filter (סינון מתקדם) נפתחת.
2. בחר את תיבת הסימון **Display only sessions within specified date range** (הצג הפעלות בטווח התאריכים שצוין בלבד).
3. בתיבות הטקסט **From date** (מתאריך) ו-**To date** (עד תאריך), הזן את היום, החודש ו/או השנה או לחץ על החץ ליד לוח השנה כדי לבחור את התאריכים.
4. לחץ על **OK** (אישור).

הצגת הפעלות שנשמרו בתיקייה שאינה תיקיית ברירת המחדל

1. ב-Live Messenger History Viewer, לחץ על סמל **Advanced Filter** (סינון מתקדם).
2. בחר את תיבת הסימון **Use an alternate history files folder** (השתמש בתיקייה חלופית של קובצי היסטוריה).

3. הזן את מיקום התיקייה או לחץ על **Browse** (עיון) כדי לחפש את התיקייה.

4. לחץ על **OK** (אישור).

משימות מתקדמות

העברת Privacy Manager Certificates (אישורים של מנהל הפרטיות) ו-Trusted Contacts (אנשי קשר מהימנים) למחשב אחר

באפשרותך להעביר בבטחה את האישורים ואנשי הקשר המהימנים של Privacy Manager (מנהל הפרטיות) למחשב אחר, או לגבות את הנתונים כדי לשמור עליהם. לשם כך, גבה את הנתונים בקובץ המוגן באמצעות סיסמה במיקום ברשת או בהתקן אחסון נשלף כלשהו, ולאחר מכן שחזר את הקובץ במחשב החדש.

גיבוי אישורים ואנשי קשר מהימנים של Privacy Manager (מנהל הפרטיות)

כדי לגבות את האישורים ואנשי הקשר המהימנים של Privacy Manager (מנהל הפרטיות) בקובץ המוגן באמצעות סיסמה, בצע את השלבים הבאים:

1. פתח את Privacy Manager (מנהל הפרטיות) ולחץ על **Migration** (העברה).
2. לחץ על **Backup** (גיבוי).
3. בדף Select Data (בחירת נתונים), בחר את קטגוריות הנתונים להכללה בקובץ ההעברה ולאחר מכן לחץ על **Next** (הבא).
4. בדף Migration File (קובץ העברה), הזן שם קובץ או לחץ על **Browse** (עיון) כדי לחפש מיקום, ולאחר מכן לחץ על **Next** (הבא).
5. הזן ואשר את הסיסמה ולאחר מכן לחץ על **Next** (הבא).

הערה: אחסן סיסמה זו במקום בטוח משום שתזדקק לה בעת שחזור קובץ ההעברה.

6. בצע אימות באמצעות שיטת הכניסה המאובטחת שבחרת.
7. בדף Migration File Saved (קובץ העברה נשמר), לחץ על **Finish** (סיום).

שחזור אישורים ואנשי קשר מהימנים של Privacy Manager (מנהל הפרטיות)

כדי לשחזר אישורים ואנשי קשר מהימנים של Privacy Manager (מנהל הפרטיות) במחשב אחר כחלק מתהליך העברה או באותו המחשב, בצע את השלבים הבאים:

1. פתח את Privacy Manager (מנהל הפרטיות) ולחץ על **Migration** (העברה).
2. לחץ על **Restore** (שחזר).
3. בדף Migration File (קובץ העברה), לחץ על **Browse** (עיון) כדי לחפש את הקובץ ולאחר מכן לחץ על **Next** (הבא).
4. הזן את הסיסמה שבה השתמשת בעת יצירת קובץ הגיבוי ולאחר מכן לחץ על **Next** (הבא).
5. בדף Migration File (קובץ העברה), לחץ על **Finish** (סיום).

הניהול המרכזי של Privacy Manager (מנהל הפרטיות)

ההתקנה של Privacy Manager (מנהל הפרטיות) עשויה להיות חלק מהתקנה מרכזית, שהותאמה אישית על-ידי מנהל המערכת. מאפיין אחד או יותר מהמאפיינים הבאים עשוי להיות מופעל או מושבת:

- **מדיניות שימוש באישורים** - ייתכן שתהיה מוגבל לשימוש באישורי Privacy Manager (מנהל הפרטיות) שהונפקו על-ידי Comodo, או שתהיה רשאי להשתמש באישורים דיגיטליים שהונפקו על-ידי רשויות אישורים אחרות.
- **מדיניות הצפנה** - ייתכן שיכולות הצפנה יופעלו או יושבתו בנפרד ב-Microsoft Office או ב-Outlook וב-Windows Live Messenger.

File Sanitizer for HP ProtectTools 10

File Sanitizer (מנקה הקבצים) הוא כלי המאפשר לך לגרוס נכסים בבטחה (מידע או קבצים אישיים, נתונים היסטוריים או הקשורים לאינטרנט או רכיבי נתונים אחרים) במחשב ולהלבין מעת לעת את הכונן הקשיח.

הערה: גרסה זו של File Sanitizer (מנקה הקבצים) תומכת בכונן הקשיח של המערכת בלבד.

גריסה

גריסה היא פעולה שונה מהמחיקה הסטנדרטית של ®Windows (המוכרת גם כמחיקה פשוטה ב-File Sanitizer (מנקה הקבצים)) משום שבעת גריסת נכס באמצעות File Sanitizer, מופעל אלגוריתם המערפל את הנתונים ומונע למעשה את האחזור של הנכס המקורי. מחיקה פשוטה של Windows עשויה להשאיר את הקובץ (או הנכס) ללא פגע בכונן הקשיח, או במצב שבו שיטות זיהוי יוכלו לשמש לשחזור הקובץ (או הנכס).

בעת בחירת פרופיל גריסה (אבטחה גבוהה, אבטחה בינונית או אבטחה נמוכה), רשימת נכסים ושיטת מחיקה מוגדרות מראש נבחרות באופן אוטומטי עבור הגריסה. באפשרותך גם להתאים אישית פרופיל גריסה, דבר המאפשר לך לציין את מספר מחזורי הגריסה, הנכסים שייכללו בגריסה, הנכסים לאישור לפני הגריסה והנכסים שלא ייכללו בגריסה. לקבלת מידע נוסף, עיין בסעיף בחירה או יצירה של פרופיל גריסה בעמוד 68.

באפשרותך להגדיר לוח זמנים אוטומטי לגריסה, ובאפשרותך גם לגרוס נכסים באופן ידני בכל עת. לקבלת מידע נוסף, ראה הגדרת לוח זמנים לגריסה בעמוד 67, גריסה ידנית של נכס אחד בעמוד 71 או גריסה ידנית של כל הפריטים שנבחרו בעמוד 71.

הערה: קובצי dll. נגרסים ומוסרים מהמערכת רק אם הועברו קודם לסל המיחזור.

הלבנת שטח פנוי

מחיקת נכס ב-Windows אינה מסירה לחלוטין את תוכן הנכס מהכונן הקשיח. Windows מוחק רק את ההפניה לנכס. תוכן הנכס נשאר בכונן הקשיח עד שנכס אחר מחליף את אותו השטח בכונן הקשיח במידע חדש.

הלבנת שטח פנוי מאפשרת לך לכתוב נתונים אקראיים בבטחה על-גבי נכסים שנמחקו, מה שמונע ממשתמשים להציג את התוכן המקורי של הנכס שנמחק.

הערה: הלבנת שטח פנוי נועדה לנכסים שמחקת באמצעות סל המיחזור של Windows או שמחקת באופן ידני. הלבנת שטח פנוי אינה מספקת אבטחה נוספת לנכסים שנגרסו.

באפשרותך להגדיר לוח זמנים אוטומטי להלבנת שטח פנוי, או להפעיל את ההלבנה באופן ידני באמצעות סמל **HP ProtectTools** באזור ההודעות, בקצה הימני או השמאלי של שורת המשימות. לקבלת מידע נוסף, ראה הגדרת לוח זמנים להלבנת שטח פנוי בעמוד 67 או הפעלה ידנית של הלבנת שטח פנוי בעמוד 72.

הליכי הגדרה

פתיחת File Sanitizer (מנקה הקבצים)

כדי לפתוח את File Sanitizer (מנקה הקבצים):

1. לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), לחץ על **HP** ולאחר מכן לחץ על **HP ProtectTools Security Manager**.
2. לחץ על **File Sanitizer** (מנקה הקבצים).

- לחלופין -

▲ לחץ לחיצה כפולה על סמל **File Sanitizer** (מנקה הקבצים) הממוקם בשולחן העבודה.

- לחלופין -

▲ לחץ לחיצה ימנית על סמל **HP ProtectTools** באזור ההודעות בקצה הימני או השמאלי של שורת המשימות, לחץ על **File Sanitizer** (מנקה הקבצים) ולאחר מכן לחץ על **Open File Sanitizer** (פתח את מנקה הקבצים).

הגדרת לוח זמנים לגריסה

הערה: לקבלת מידע על בחירת פרופיל גריסה מוגדר מראש או על יצירת פרופיל גריסה, ראה בחירה או יצירה של פרופיל גריסה בעמוד 68.

הערה: לקבלת מידע על גריסה ידנית של נכסים, ראה גריסה ידנית של נכס אחד בעמוד 71.

1. פתח את File Sanitizer (מנקה הקבצים) ולחץ על **Shred** (גריסה).
2. בחר אפשרות גריסה:
   - **Windows shutdown** (כיבוי Windows) - בחר אפשרות זו כדי לגרוס את כל הנכסים שנבחרו בעת כיבוי Windows.

     הערה: כאשר אפשרות זו נבחרת, תיבת דו-שיח מוצגת במהלך הכיבוי ושואלת אם ברצונך להמשיך בגריסה של הנכסים שנבחרו או אם ברצונך לעקוף את ההליך. לחץ על **Yes** (כן) כדי לעקוף את הליך הגריסה או לחץ על **No** (לא) כדי להמשיך בגריסה.

   - **Web browser open** (פתיחת דפדפן אינטרנט) - בחר אפשרות זו כדי לגרוס את כל הנכסים הקשורים לאינטרנט שנבחרו, כגון היסטוריית כתובות URL שאליהן גלשת, בעת פתיחת דפדפן אינטרנט.
   - **Web browser quit** (יציאה מדפדפן אינטרנט) - בחר אפשרות זו כדי לגרוס את כל הנכסים הקשורים לאינטרנט שנבחרו, כגון היסטוריית כתובות URL שאליהן גלשת, בעת סגירת דפדפן אינטרנט.
   - **Key sequence** (רצף מקשים) - בחר אפשרות זו כדי להפעיל גריסה באמצעות רצף מקשים.
   - **Scheduler** (מתזמן) - בחר את תיבת הסימון **Activate Scheduler** (הפעל מתזמן), הזן את סיסמת Windows ולאחר מכן הזן יום ושעה לגריסת הנכסים שנבחרו.

   הערה: קובצי dll. נגרסים ומוסרים מהמערכת רק אם הועברו קודם לסל המיחזור.

3. לחץ על **Apply** (החל) ולאחר מכן לחץ על **OK** (אישור).

הגדרת לוח זמנים להלבנת שטח פנוי

הערה: הלבנת שטח פנוי נועדה לנכסים שמחקת באמצעות סל המיחזור של Windows או עבור נכסים שנמחקו ידנית. הלבנת שטח פנוי אינה מספקת אבטחה נוספת לנכסים שנגרסו.

כדי להגדיר לוח זמנים להלבנת שטח פנוי:

1. פתח את File Sanitizer (מנקה הקבצים) ולחץ על **Free Space Bleaching** (הלבנת שטח פנוי).
2. בחר את תיבת הסימון **Activate Scheduler** (הפעל מתזמן), הזן את סיסמת Windows ולאחר מכן הזן יום ושעה להלבנת הכונן הקשיח.
3. לחץ על **Apply** (החל) ולאחר מכן לחץ על **OK** (אישור).

הערה: פעולת הלבנת השטח הפנוי עשויה להימשך זמן רב. למרות שהלבנת שטח פנוי מבוצעת ברקע, המחשב עלול להאט את פעולתו עקב שימוש מוגבר במעבד.

בחירה או יצירה של פרופיל גריסה

באפשרותך לציין שיטה למחיקה ולבחור את הנכסים לגריסה על-ידי בחירת פרופיל מוגדר מראש או יצירת פרופיל משלך.

בחירת פרופיל גריסה מוגדר מראש

בעת בחירת פרופיל גריסה מוגדר מראש (אבטחה גבוהה, אבטחה בינונית או אבטחה נמוכה), שיטת מחיקה ורשימת נכסים מוגדרות מראש נבחרות באופן אוטומטי. באפשרותך ללחוץ על הלחצן **View Details** (הצג פרטים) כדי להציג את הרשימה המוגדרת מראש של הנכסים שנבחרו לגריסה.

כדי לבחור פרופיל גריסה מוגדר מראש:

1. פתח את File Sanitizer (מנקה הקבצים) ולחץ על **Settings** (הגדרות).
2. לחץ על פרופיל גריסה מוגדר מראש.
3. לחץ על **View Details** (הצג פרטים) כדי להציג את רשימת הנכסים שנבחרו לגריסה.
4. תחת **Shred the following** (גרוס את הבאים), בחר בתיבת הסימון ליד כל נכס שאותו ברצונך לאשר לפני גריסה.
5. לחץ על **Apply** (החל) ולאחר מכן לחץ על **OK** (אישור).

התאמה אישית של פרופיל גריסה

בעת יצירת פרופיל גריסה, באפשרותך לציין את מספר מחזורי הגריסה, הנכסים שייכללו בגריסה, הנכסים שיש לאשר לפני הגריסה והנכסים שלא ייכללו בגריסה:

1. פתח את File Sanitizer (מנקה הקבצים) ולחץ על **Settings** (הגדרות), לחץ על **Advanced Security Settings** (הגדרות אבטחה מתקדמות) ולאחר מכן לחץ על **View Details** (הצג פרטים).
2. ציין את מספר מחזורי הגריסה.

הערה: מספר מחזורי הגריסה שנבחר יבוצע עבור כל נכס. לדוגמה, אם תבחר 3 מחזורי גריסה, אלגוריתם המערפל את הנתונים יבוצע 3 פעמים. אם תבחר מחזורי גריסה עם אבטחה גבוהה יותר, הגריסה עשויה להימשך זמן רב; עם זאת, ככל שתציין מספר גבוה יותר של מחזורי גריסה, כך פוחת הסיכוי לאחזור הנתונים.

3. בחר את הנכסים שברצונך לגרוס:

   א. תחת **Available shred options** (אפשרויות גריסה זמינות), לחץ על נכס ולאחר מכן לחץ על **Add** (הוסף).

   ב. כדי להוסיף נכס מותאם אישית, לחץ על **Add Custom Option** (הוסף אפשרות מותאמת אישית) ולאחר מכן אתר או הקלד את הנתיב לשם הקובץ או התיקייה. לחץ על **Open** (פתח) ולאחר מכן לחץ על **OK** (אישור). תחת **Available shred options** (אפשרויות גריסה זמינות), לחץ על הנכס המותאם אישית ולאחר מכן לחץ על **Add** (הוסף).

הערה: כדי להסיר נכס מאפשרויות הגריסה הזמינות, לחץ על הנכס ולאחר מכן לחץ על **Delete** (מחק).

4. תחת **Shred the following** (גרוס את הבאים), בחר את תיבת הסימון ליד כל נכס שברצונך לאשר לפני הגריסה.

הערה: להסרת נכס מרשימת הגריסה, לחץ על הנכס ולאחר מכן לחץ על **Remove** (הסר).

5. כדי להגן על קבצים או תיקיות מפני גריסה אוטומטית, תחת **Do not shred the following** (אל תגרוס את הפריטים הבאים), לחץ על **Add** (הוסף) ולאחר מכן אתר או הקלד את הנתיב לשם הקובץ או התיקייה. לחץ על **Open** (פתח) ולאחר מכן לחץ על **OK** (אישור).

הערה: להסרת נכס מרשימת הנכסים שאין לכלול בגריסה, לחץ על הנכס ולאחר מכן לחץ על **Delete** (מחק).

6. כשתסיים להגדיר את פרופיל הגריסה, לחץ על **Apply** (החל) ולאחר מכן לחץ על **OK** (אישור).

התאמה אישית של פרופיל מחיקה פשוטה

פרופיל המחיקה הפשוטה מבצע מחיקה רגילה של נכס ללא גריסה. בעת התאמה אישית של פרופיל מחיקה פשוטה, אתה מציין את הנכסים שייכללו במחיקה הפשוטה, הנכסים לאישור לפני ביצוע המחיקה הפשוטה והנכסים שלא ייכללו במחיקה הפשוטה.

הערה: אם אתה משתמש באפשרות המחיקה הפשוטה, הלבנה של שטח פנוי יכולה להתבצע מעת לעת בנכסים שנמחקו ידנית או באמצעות סל המיחזור של Windows.

כדי להתאים אישית פרופיל מחיקה פשוטה:

1. פתח את File Sanitizer (מנקה הקבצים), לחץ על **Settings** (הגדרות), לחץ על **Simple Delete Setting** (הגדרת מחיקה פשוטה) ולאחר מכן לחץ על **View Details** (הצג פרטים).

2. בחר בנכסים שאותם ברצונך למחוק:

   א. תחת **Available delete options** (אפשרויות מחיקה זמינות), לחץ על נכס ולאחר מכן לחץ על **Add** (הוסף).

   ב. כדי להוסיף נכס מותאם אישית, לחץ על **Add Custom Option** (הוסף אפשרות מותאמת אישית), הזן שם קובץ או שם תיקייה ולאחר מכן לחץ על **OK** (אישור). לחץ על הנכס המותאם אישית ולאחר מכן לחץ על **Add** (הוסף).

הערה: כדי למחוק נכס מאפשרויות המחיקה הזמינות, לחץ על הנכס ולאחר מכן לחץ על **Delete** (מחק).

3. תחת **Delete the following** (מחק את הבאים), בחר את תיבת הסימון ליד כל נכס שאותו ברצונך לאשר לפני מחיקה.

הערה: להסרת נכס מרשימת המחיקה, לחץ על הנכס ולאחר מכן לחץ על **Remove** (הסר).

4. תחת **Do not delete the following** (אל תמחק את הבאים), לחץ על **Add** (הוסף) כדי לבחור את הנכסים הספציפיים שאין ברצונך לכלול במחיקה.

הערה: להסרת נכס מרשימת הנכסים שאין לכלול, לחץ על הנכס ולאחר מכן לחץ על **Delete** (מחק).

5. כשתסיים להגדיר את פרופיל המחיקה הפשוטה, לחץ על **Apply** (החל) ולאחר מכן לחץ על **OK** (אישור).

משימות כלליות

באפשרותך להשתמש ב-File Sanitizer (מנקה הקבצים) לביצוע המשימות הבאות:

- שימוש ברצף מקשים להפעלת גריסה - מאפיין זה מאפשר לך ליצור רצף מקשים (לדוגמה, ctrl+alt+s) להפעלת גריסה. לקבלת פרטים, ראה שימוש ברצף מקשים להפעלת גריסה בעמוד 70.
- שימוש בסמל File Sanitizer (מנקה הקבצים) להפעלת גריסה - מאפיין זה דומה למאפיין הגרירה והשחרור ב-Windows. לקבלת פרטים, ראה שימוש בסמל File Sanitizer (מנקה הקבצים) בעמוד 71.
- גריסה ידנית של נכס ספציפי או של כל הנכסים שנבחרו - מאפיינים אלה מאפשרים לך לגרוס פריטים באופן ידני מבלי להמתין להפעלת לוח הזמנים הרגיל לגריסה. לקבלת פרטים, ראה גריסה ידנית של נכס אחד בעמוד 71 או גריסה ידנית של כל הפריטים שנבחרו בעמוד 71.
- הפעלה ידנית של הלבנת שטח פנוי - מאפיין זה מאפשר לך להפעיל ידנית את הלבנת השטח הפנוי. לקבלת פרטים, ראה הפעלה ידנית של הלבנת שטח פנוי בעמוד 72.
- ביטול פעולה של גריסה או הלבנת שטח פנוי - מאפיין זה מאפשר לך לעצור פעולה של גריסה או הלבנת שטח פנוי. לקבלת פרטים, ראה ביטול פעולה של גריסה או הלבנת שטח פנוי בעמוד 72.
- הצגת קובצי היומן - מאפיין זה מאפשר לך להציג קובצי יומן של גריסה והלבנת שטח פנוי, המכילים שגיאות או כשלים מהפעולה האחרונה של הגריסה או הלבנת השטח הפנוי. לקבלת פרטים, ראה הצגת קובצי היומן בעמוד 72.

הערה: פעולת הגריסה או הלבנת השטח הפנוי עשויה להימשך זמן רב. למרות שהלבנת שטח פנוי וגריסה מבוצעות ברקע, המחשב עשוי להאט את פעולתו עקב שימוש מוגבר במעבד.

שימוש ברצף מקשים להפעלת גריסה

כדי לציין רצף מקשים, בצע את השלבים הבאים:

1. פתח את File Sanitizer (מנקה הקבצים) ולחץ על **Shred** (גריסה).
2. בחר את תיבת הסימון **Key sequence** (רצף מקשים).
3. הזן תו בתיבת הטקסט.
4. בחר בתיבת הסימון **CTRL** או בתיבת הסימון **ALT**, ולאחר מכן בחר בתיבה **SHIFT**.

לדוגמה, כדי להפעיל גריסה אוטומטית באמצעות מקש s ו-ctrl+shift, הזן את התו s בתיבת הטקסט, ולאחר מכן בחר את תיבות הסימון **CTRL** ו-**SHIFT**.

הערה: הקפד לבחור רצף מקשים שאינו דומה לכל רצף מקשים אחר שהגדרת.

כדי להפעיל גריסה באמצעות רצף מקשים:

1. לחץ לחיצה ממושכת על מקש shift ועל מקש ctrl או מקש alt (או כל שילוב אחר שציינת) בעת הקשה על התו שבחרת.
2. אם נפתחת תיבת דו-שיח לאישור, לחץ על **Yes** (כן).

שימוש בסמל File Sanitizer (מנקה הקבצים)

△ **זהירות:** אין אפשרות לשחזר נכסים שנגרסו. חשוב היטב על הפריטים שאתה בוחר לגריסה ידנית.

1. נווט אל המסמך או התיקייה שברצונך לגרוס.
2. גרור את הנכס אל סמל **מנקה הקבצים** בשולחן העבודה.
3. כאשר נפתחת תיבת הדו-שיח לאישור, לחץ על **Yes** (כן).

גריסה ידנית של נכס אחד

△ **זהירות:** אין אפשרות לשחזר נכסים שנגרסו. חשוב היטב על הפריטים שאתה בוחר לגריסה ידנית.

1. לחץ לחיצה ימנית על סמל **HP ProtectTools** באזור ההודעות בקצה הימני או השמאלי של שורת המשימות, לחץ על **File Sanitizer** (מנקה הקבצים) ולאחר מכן לחץ על **Shred One** (גרוס פריט אחד).
2. בעת הופעת תיבת הדו-שיח Browse (עיון), נווט אל הנכס שברצונך לגרוס ולאחר מכן לחץ על **OK** (אישור).

הערה: הנכס שאתה בוחר יכול להיות קובץ בודד או תיקייה.

3. כאשר נפתחת תיבת הדו-שיח לאישור, לחץ על **Yes** (כן).

- לחלופין -

1. לחץ לחיצה ימנית על סמל **File Sanitizer** (מנקה הקבצים) בשולחן העבודה ולאחר מכן לחץ על **Shred One** (גרוס פריט אחד).
2. בעת הופעת תיבת הדו-שיח Browse (עיון), נווט אל הנכס שברצונך לגרוס ולאחר מכן לחץ על **OK** (אישור).
3. כאשר נפתחת תיבת הדו-שיח לאישור, לחץ על **Yes** (כן).

- לחלופין -

1. פתח את File Sanitizer (מנקה הקבצים) ולחץ על **Shred** (גריסה).
2. לחץ על הלחצן **Browse** (עיון).
3. בעת הופעת תיבת הדו-שיח Browse (עיון), נווט אל הנכס שברצונך לגרוס ולאחר מכן לחץ על **OK** (אישור).
4. כאשר נפתחת תיבת הדו-שיח לאישור, לחץ על **Yes** (כן).

גריסה ידנית של כל הפריטים שנבחרו

1. לחץ לחיצה ימנית על סמל **HP ProtectTools** באזור ההודעות בקצה הימני או השמאלי של שורת המשימות, לחץ על **File Sanitizer** (מנקה הקבצים) ולאחר מכן לחץ על **Shred Now** (גרוס כעת).
2. כאשר נפתחת תיבת הדו-שיח לאישור, לחץ על **Yes** (כן).

- לחלופין -

1. לחץ לחיצה ימנית על סמל **File Sanitizer** (מנקה הקבצים) בשולחן העבודה ולאחר מכן לחץ על **Shred Now** (גרוס כעת).
2. כאשר נפתחת תיבת הדו-שיח לאישור, לחץ על **Yes** (כן).

- לחלופין -

1. פתח את File Sanitizer (מנקה הקבצים) ולחץ על **Shred** (גריסה).
2. לחץ על הלחצן **Shred now** (גרוס כעת).
3. כאשר נפתחת תיבת הדו-שיח לאישור, לחץ על **Yes** (כן).

הפעלה ידנית של הלבנת שטח פנוי

1. לחץ לחיצה ימנית על סמל **HP ProtectTools** באזור ההודעות בקצה הימני או השמאלי של שורת המשימות, לחץ על **File Sanitizer** (מנקה הקבצים) ולאחר מכן לחץ על **Bleach Now** (הלבן כעת).
2. כאשר נפתחת תיבת הדו-שיח לאישור, לחץ על **Yes** (כן).

- לחלופין -

1. פתח את File Sanitizer (מנקה הקבצים) ולחץ על **Free Space Bleaching** (הלבנת שטח פנוי).
2. לחץ על **Bleach Now** (הלבן כעת).
3. כאשר נפתחת תיבת הדו-שיח לאישור, לחץ על **Yes** (כן).

ביטול פעולה של גריסה או הלבנת שטח פנוי

כאשר מתבצעת פעולה של גריסה או הלבנת שטח פנוי, מוצגת הודעה מעל סמל HP ProtectTools Security Manager באזור ההודעות. ההודעה מספקת פרטים על תהליך הגריסה או הלבנת השטח הפנוי (אחוז ביצוע) ומאפשרת לך לבטל את הפעולה.

כדי לבטל את הפעולה:

▲ לחץ על ההודעה ולאחר מכן לחץ על **Stop** (עצור) כדי לבטל את הפעולה.

הצגת קובצי היומן

בכל פעם שמתבצעת פעולה של גריסה או הלבנת שטח פנוי, נוצרים קובצי יומן המכילים כל שגיאה או כשל שהתרחשו. קובצי היומן תמיד מעודכנים בהתאם לפעולה האחרונה של הגריסה או הלבנת השטח הפנוי.

הערה: קבצים שנגרסו או הולבנו בהצלחה אינם מופיעים בקובצי היומן.

קובץ יומן אחד נוצר עבור פעולות גריסה, וקובץ אחר נוצר עבור פעולות של הלבנת שטח פנוי. שני קובצי היומן ממוקמים בכונן הקשיח תחת:

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

11 Device Access Manager for HP ProtectTools (בדגמים נבחרים בלבד)

מנהלי מערכת ההפעלה ®Windows משתמשים ב-Device Access Manager for HP ProtectTools לבקרת גישה להתקנים במערכת ולהגנה מפני גישה בלתי מורשית:

- פרופילי התקן נוצרים עבור כל משתמש כדי להגדיר את ההתקנים שיש או אין לו גישה אליהם.
- משתמשים גם מאורגנים בקבוצות, כגון הקבוצה המוגדרת מראש Device Administrator (מנהלי התקנים), וניתן להגדיר קבוצות באמצעות האפשרות Computer Management (ניהול המחשב) במקטע Administrative Tools (כלי ניהול) של לוח הבקרה.
- ניתן להעניק או לחסום גישה להתקן בהתבסס על חברות בקבוצה.
- עבור מחלקות התקנים כגון כונני תקליטורים ו-DVD, ניתן להעניק או לחסום גישת קריאה וגישת כתיבה בנפרד.

כמו כן, ניתן להעניק למספר משתמשים מוגבל את ההרשאה לקרוא ולשנות את מדיניות בקרת הגישה של ההתקנים.

הליכי הגדרה

פתיחת Device Access Manager (מנהל הגישה להתקנים)

כדי לפתוח את Device Access Manager (מנהל הגישה להתקנים)

1. לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), לחץ על **HP** ולאחר מכן לחץ על **HP ProtectTools Administrative Console**.
2. בחלונית השמאלית או הימנית, לחץ על **Device Access Manager** (מנהל הגישה להתקנים).

הגדרת תצורה של גישה להתקנים

Device Access Manager for HP ProtectTools מציע שלוש תצוגות:

- התצוגה Simple Configuration (תצורה פשוטה) משמשת להרשאה או לחסימה של גישה למחלקות התקנים עבור חברים בקבוצה Device Administrator (מנהלי התקנים).
- התצוגה Device Class Configuration (תצורת מחלקות התקנים) משמשת להרשאה או לחסימה של גישה לסוגי התקנים או להתקנים ספציפיים עבור משתמשים ספציפיים או קבוצות.
- התצוגה User Access Settings (הגדרות גישת משתמשים) משמשת לציון המשתמשים שיוכלו להציג או לשנות את המידע בתצוגות Simple Configuration (תצורה פשוטה) ו-Device Class Configuration (תצורת מחלקות התקנים).

הקבוצה Device Administrators (מנהלי התקנים)

בעת התקנת Device Access Manager (מנהל הגישה להתקנים), נוצרת קבוצה בשם Device Administrators (מנהלי התקנים).

מנהל המערכת יכול ליישם מדיניות פשוטה של בקרת גישה להתקנים על-ידי חסימת גישה לסדרה של מחלקות התקנים, אלא אם משתמש מוגדר כמשתמש מהימן (מבחינת הגישה להתקנים). הדרך המומלצת להבחנה בין משתמשים מהימנים ובלתי מהימנים "מבחינת התקנים" היא להפוך את כל המשתמשים המהימנים לחברים בקבוצה Device Administrators (מנהלי התקנים). לפיכך, הענקת גישה להתקנים לחברי הקבוצה Device Administrators (מנהלי התקנים) באמצעות התצוגות Simple Configuration (תצורה פשוטה) או Device Class Configuration (תצורת מחלקות התקנים) תבטיח שמשתמשים "מהימנים להתקן" יזכו לגישה מלאה לסדרה שצוינה של מחלקות התקנים.

הערה: הוספת משתמש לקבוצה Device Administrators (מנהלי התקנים) אינה מאפשרת למשתמש לגשת להתקנים באופן אוטומטי. עם זאת, ניתן להשתמש בתצוגה Simple Configuration (תצורה פשוטה) כדי להעניק גישה לסדרת מחלקות ההתקנים הרצויה עבור משתמשים "מהימנים להתקן".

כדי להוסיף משתמשים לקבוצה Device Administrators (מנהלי התקנים), בצע את השלבים הבאים:

- עבור Windows 7, Vista או XP Professional, השתמש ביישום ה-Snap-in הרגיל של MMC, Local Users and Groups (משתמשים וקבוצות מקומיים).
- עבור גרסאות ביתיות של Windows 7, Vista® או XP, מחשבון בעל זכויות, הקלד את הטקסט הבא בחלון שורת הפקודה:

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

Simple Configuration (תצורה פשוטה)

מנהלי מערכת ומשתמשים מורשים יכולים להשתמש בתצוגה Simple Configuration (תצורה פשוטה) כדי לשנות גישה למחלקות ההתקנים הבאות עבור כל המשתמשים שאינם מנהלי התקנים:

הערה: כדי להשתמש בתצוגה זו לקריאת מידע על גישה להתקנים, יש להעניק למשתמש או לקבוצה גישת "קריאה" בתצוגה **User Access Settings** (הגדרות גישת משתמשים). כדי להשתמש בתצוגה זו לשינוי מידע על גישה להתקנים, יש להעניק למשתמש או לקבוצה גישת "שינוי" בתצוגה **User Access Settings** (הגדרות גישת משתמשים).

- כל המדיה הנשלפת (תקליטונים, כונני USB flash וכולי)
- כל כונני ה-CD/DVD
- כל היציאות הטוריות והמקביליות
- כל התקני Bluetooth®
- כל התקני האינפרה-אדום
- כל התקני המודם
- כל התקני ה-PCMCIA
- כל התקני ה-1394

כדי לאפשר או לחסום גישה למחלקת התקנים עבור כל המשתמשים שאינם מנהלי התקנים, בצע את השלבים הבאים:

1. בחלונית השמאלית או הימנית של **HP ProtectTools Administrative Console**, לחץ על **Device Access Manager** (מנהל הגישה להתקנים) ולאחר מכן לחץ על **Simple Configuration** (תצורה פשוטה).
2. בחלונית הימנית או השמאלית, כדי לחסום גישה, בחר את תיבת הסימון של מחלקת התקנים או התקן ספציפי. נקה את תיבת הסימון כדי לאפשר גישה לאותה מחלקת התקנים או לאותו התקן ספציפי.

   אם תיבת הסימון אפורה, הערכים שמשפיעים על תרחיש הגישה השתנו מתוך התצוגה Device Class Configuration (תצורת מחלקות התקנים). כדי לאפס את הערכים חזרה להגדרות הפשוטות, לחץ על תיבת הסימון כדי לנקות אותה או להגדיר אותה, ולאחר מכן לחץ על **Yes** (כן) כדי לאשר.
3. לחץ על המסך **Save** (שמור).

   הערה: אם שירות ברקע אינו מופעל, נפתחת תיבת דו-שיח ששואלת אם ברצונך להפעיל אותו. לחץ על **Yes** (כן).
4. לחץ על **OK** (אישור).

הפעלת שירות ברקע

לפני שניתן להחיל פרופילי התקן, HP ProtectTools Security Manager פותח תיבת דו-שיח ששואלת אם ברצונך להפעיל את השירות ברקע HP ProtectTools Device Locking/Auditing. לחץ על **Yes** (כן). השירות ברקע מופעל ולכן יופעל באופן אוטומטי בכל אתחול של המערכת.

הערה: יש להגדיר פרופיל התקן לפני הצגת הבקשה של השירות ברקע.

מנהלי מערכת יכולים גם כן להפעיל או להפסיק שירות זה:

1. לחץ על **Start** (התחל) ולאחר מכן לחץ על **Control Panel** (לוח הבקרה).
2. לחץ על **Administrative Tools** (כלי ניהול) ולאחר מכן לחץ על **Services** (שירותים).
3. חפש את השירות **HP ProtectTools Device Locking/Auditing**.

הפסקת השירות Device Locking/Auditing (נעילת התקנים/ביקורת) אינה מפסיקה את נעילת ההתקן. שני רכיבים כופים נעילת התקנים:

- שירות Device Locking/Auditing (נעילת התקנים/ביקורת)
- מנהל ההתקן DAMDrv.sys

הפעלת השירות מפעילה את מנהל ההתקן, אך הפסקת השירות אינה מפסיקה את מנהל ההתקן.

כדי לקבוע אם השירות ברקע פועל, פתח חלון של שורת הפקודה והקלד sc query flcdlock.

כדי לקבוע אם מנהל ההתקן פועל, פתח חלון של שורת הפקודה והקלד sc query damdrv.

Device Class Configuration (תצורת מחלקות התקנים)

מנהלי מערכת ומשתמשים מורשים יכולים להציג ולשנות רשימות של משתמשים וקבוצות שיש או אין להם גישה למחלקות התקנים או להתקנים ספציפיים.

הערה: כדי להשתמש בתצוגה זו לקריאת מידע על גישה להתקנים, יש להעניק למשתמש או לקבוצה גישת "קריאה" בתצוגה **User Access Settings** (הגדרות גישת משתמשים). כדי להשתמש בתצוגה זו לשינוי מידע על גישה להתקנים, יש להעניק למשתמש או לקבוצה גישת "שינוי" בתצוגה **User Access Settings** (הגדרות גישת משתמשים).

התצוגה Device Class Configuration (תצורת מחלקות התקנים) כוללת את המקטעים הבאים:

- **Device List** (רשימת התקנים) - הרשימה מציגה את כל מחלקות ההתקנים וההתקנים המותקנים במערכת, או שייתכן שהותקנו במערכת בעבר.
  - ניתן בדרך כלל להחיל הגנה על מחלקות התקנים. משתמש או קבוצה שנבחרו יוכלו לגשת לכל התקן ברשימת ההתקנים.
  - ניתן גם להחיל הגנה על התקנים ספציפיים.
- **User List** (רשימת משתמשים) - הרשימה מציגה את כל המשתמשים והקבוצות שיש או אין להם גישה למחלקת ההתקנים או להתקן הספציפי שנבחרו.
  - ניתן להוסיף רישום לרשימת המשתמשים של משתמש ספציפי או קבוצה שבה חבר המשתמש.
  - אם רישום של משתמש או קבוצה ברשימת המשתמשים אינו זמין, ההגדרה עברה בירושה ממחלקת ההתקנים ברשימת ההתקנים או מתיקיית המחלקות.
  - מחלקות התקנים מסוימות, כגון התקני CD/DVD, מאפשרות שליטה נוספת על-ידי מתן גישה או חסימת גישה לפעולות קריאה וכתיבה בנפרד.

  בהתקנים ומחלקות אחרים, ניתן לקבל בירושה זכויות גישה של קריאה וכתיבה. לדוגמה, ניתן לקבל זכות קריאה בירושה ממחלקה גבוהה יותר, אך ניתן לחסום גישת כתיבה באופן ספציפי עבור משתמש או קבוצה.

  הערה: אם תיבת הסימון Read (קריאה) ריקה, רישום בקרת הגישה אינו משפיע על גישת קריאה להתקן. הוא אינו מעניק או חוסם גישת קריאה להתקן.

  דוגמה 1 - אם למשתמש או לקבוצה אין גישת כתיבה להתקן או למחלקת התקנים:

  אותו משתמש, אותה קבוצה או חבר באותה קבוצה יכולים לקבל גישת כתיבה או גישת קריאה+כתיבה רק עבור התקן שנמצא מתחת להתקן זה בהיררכיית ההתקנים.

  דוגמה 2 - אם למשתמש או לקבוצה יש גישת כתיבה להתקן או למחלקת התקנים:

  אותו משתמש, אותה קבוצה או חבר באותה קבוצה יכולים שלא לקבל גישת כתיבה או גישת קריאה+כתיבה רק עבור אותו ההתקן או התקן שנמצא מתחת להתקן זה בהיררכיית ההתקנים.

דוגמה 3 - אם למשתמש או לקבוצה יש גישת קריאה להתקן או למחלקת התקנים:

אותו משתמש, אותה קבוצה או חבר באותה קבוצה יכולים שלא לקבל גישת קריאה או גישת קריאה+כתיבה רק לאותו ההתקן או להתקן שנמצא מתחת להתקן זה בהיררכיית ההתקנים.

דוגמה 4 - אם למשתמש או לקבוצה אין גישת קריאה להתקן או למחלקת התקנים:

אותו משתמש, אותה קבוצה או חבר באותה קבוצה יכולים לקבל גישת קריאה או גישת קריאה+כתיבה רק עבור התקן מתחת להתקן זה בהיררכיית ההתקנים.

דוגמה 5 - אם למשתמש או לקבוצה יש גישת קריאה+כתיבה להתקן או למחלקת התקנים:

אותו משתמש, אותה קבוצה או חבר באותה קבוצה יכולים שלא לקבל גישת כתיבה או גישת קריאה+כתיבה רק עבור אותו ההתקן או התקן שנמצא מתחת להתקן זה בהיררכיית ההתקנים.

דוגמה 6 - אם למשתמש או לקבוצה אין גישת קריאה+כתיבה להתקן או למחלקת התקנים:

אותו משתמש, אותה קבוצה או חבר באותה קבוצה יכולים לקבל גישת קריאה או גישת קריאה+כתיבה רק עבור התקן שנמצא מתחת להתקן זה בהיררכיית ההתקנים.

חסימת גישה של משתמש או קבוצה

כדי למנוע ממשתמש או קבוצה לגשת להתקן או למחלקת התקנים, בצע את השלבים הבאים:

1. בחלונית השמאלית או הימנית של **HP ProtectTools Administrative Console**, לחץ על **Device Access Manager** (מנהל הגישה להתקנים) ולאחר מכן לחץ על **Device Class Configuration** (תצורת מחלקות התקנים).
2. ברשימת ההתקנים, לחץ על מחלקת ההתקנים שברצונך להגדיר.
   - Device class (מחלקת התקנים)
   - All devices (כל ההתקנים)
   - Individual device (התקן יחיד)
3. תחת **User/Groups** (משתמש/קבוצה), לחץ על המשתמש או הקבוצה שיש לחסום את הגישה שלהם.
4. לחץ על **Deny** (חסום) ליד משתמש או קבוצה.
5. לחץ על הסמל **Save** (שמור).

הערה: כאשר הגדרות חסימה ומתן גישה מוגדרות באותה רמת התקן עבור משתמש כלשהו, חסימת הגישה מקבלת עדיפות על-פני מתן הגישה.

מתן גישה למשתמש או קבוצה

כדי להעניק הרשאה למשתמש או לקבוצה לגשת להתקן או למחלקת התקנים, בצע את השלבים הבאים:

1. בחלונית השמאלית או הימנית של **HP ProtectTools Administrative Console**, לחץ על **Device Access Manager** (מנהל הגישה להתקנים) ולאחר מכן לחץ על **Device Class Configuration** (תצורת מחלקות התקנים).
2. ברשימת ההתקנים, לחץ על אחת מהאפשרויות הבאות:
   - Device class (מחלקת התקנים)
   - All devices (כל ההתקנים)
   - Individual device (התקן יחיד)

3. לחץ על **Add** (הוסף).

תיבת הדו-שיח **Select Users or Groups** (בחירת משתמשים או קבוצות) נפתחת.

4. לחץ על **Advanced** (מתקדם) ולאחר מכן לחץ על **Find Now** (מצא כעת) כדי לחפש אחר משתמשים או קבוצות להוספה.

5. לחץ על משתמש או קבוצה להוספה לרשימת המשתמשים והקבוצות הזמינים, ולאחר מכן לחץ על **OK** (אישור).

6. לחץ שוב על **OK** (אישור).

7. לחץ על **Allow** (אפשר) כדי להעניק גישה למשתמש זה או לקבוצה זו.

8. לחץ על הסמל **Save** (שמור).

הסרת גישה של משתמש או קבוצה

כדי להסיר הרשאה של משתמש או קבוצה לגשת להתקן או למחלקת התקנים, בצע את השלבים הבאים:

1. בחלונית השמאלית או הימנית של **HP ProtectTools Administrative Console**, לחץ על **Device Access Manager** (מנהל הגישה להתקנים) ולאחר מכן לחץ על **Device Class Configuration** (תצורת מחלקות התקנים).

2. ברשימת ההתקנים, לחץ על מחלקת ההתקנים שברצונך להגדיר.
   - Device class (מחלקת התקנים)
   - All devices (כל ההתקנים)
   - Individual device (התקן יחיד)

3. תחת **User/Groups** (משתמש/קבוצה), לחץ על המשתמש או הקבוצה שברצונך להסיר ולאחר מכן לחץ על **Remove** (הסר).

4. לחץ על הסמל **Save** (שמור).

מתן גישה למחלקת התקנים עבור משתמש אחד מתוך קבוצה

כדי לאפשר למשתמש לגשת למחלקת התקנים תוך חסימת הגישה של כל שאר החברים בקבוצה של אותו משתמש, בצע את השלבים הבאים:

1. בחלונית השמאלית או הימנית של **HP ProtectTools Administrative Console**, לחץ על **Device Access Manager** (מנהל הגישה להתקנים) ולאחר מכן לחץ על **Device Class Configuration** (תצורת מחלקות התקנים).

2. ברשימת ההתקנים, לחץ על מחלקת ההתקנים שברצונך להגדיר.
   - Device class (מחלקת התקנים)
   - All devices (כל ההתקנים)
   - Individual device (התקן יחיד)

3. תחת **User/Groups** (משתמש/קבוצה), בחר את הקבוצה לחסימת גישה ולאחר מכן לחץ על **Deny** (חסום).

4. נווט אל התיקייה מתחת לזו של המחלקה הדרושה ולאחר מכן הוסף את המשתמש הספציפי.

5. לחץ על **Allow** (אפשר) כדי להעניק גישת משתמש זו.

6. לחץ על הסמל **Save** (שמור).

הרשאת גישה להתקן ספציפי עבור משתמש אחד מתוך קבוצה

למנהלי מערכת יש אפשרות להעניק למשתמש גישה להתקן ספציפי, תוך חסימת הגישה של כל שאר החברים בקבוצה של אותו משתמש לכל ההתקנים במחלקה:

1. בחלונית השמאלית או הימנית של **HP ProtectTools Administrative Console**, לחץ על **Device Access Manager** (מנהל הגישה להתקנים) ולאחר מכן לחץ על **Device Class Configuration** (תצורת מחלקות התקנים).
2. ברשימת ההתקנים, לחץ על מחלקת ההתקנים שברצונך להגדיר ולאחר מכן נווט אל התיקייה שמתחתיה.
3. לחץ על **Add** (הוסף). תיבת הדו-שיח **Select Users or Groups** (בחירת משתמשים או קבוצות) נפתחת.
4. לחץ על **Advanced** (מתקדם) ולאחר מכן לחץ על **Find Now** (מצא כעת) כדי לחפש את קבוצת המשתמש שיש לחסום את גישתה לכל ההתקנים במחלקה.
5. לחץ על הקבוצה ולאחר מכן לחץ על **OK** (אישור).
6. נווט אל ההתקן הספציפי תחת מחלקת ההתקנים שאליו יוכל המשתמש לגשת.
7. לחץ על **Add** (הוסף). תיבת הדו-שיח **Select Users or Groups** (בחירת משתמשים או קבוצות) נפתחת.
8. לחץ על **Advanced** (מתקדם) ולאחר מכן לחץ על **Find Now** (מצא כעת) כדי לחפש אחר משתמשים או קבוצות להוספה.
9. לחץ על המשתמש שיקבל את הגישה ולאחר מכן לחץ על **OK** (אישור).
10. לחץ על **Allow** (אפשר) כדי להעניק גישת משתמש זו.
11. לחץ על הסמל **Save** (שמור).

איפוס התצורה

△ **זהירות:** איפוס התצורה מוחק את כל השינויים שבוצעו בתצורת ההתקנים ומחזיר את כל ההגדרות לערכים שהגדיר היצרן.

כדי לאפס את הגדרות התצורה לערכי היצרן, בצע את השלבים הבאים:

1. בחלונית השמאלית או הימנית של **HP ProtectTools Administrative Console**, לחץ על **Device Access Manager** (מנהל הגישה להתקנים) ולאחר מכן לחץ על **Device Class Configuration** (תצורת מחלקות התקנים).
2. לחץ על הלחצן **Reset** (איפוס).
3. לחץ על **Yes** (כן) כדי לאשר.
4. לחץ על הסמל **Save** (שמור).

משימות מתקדמות

בקרת גישה להגדרות התצורה

בתצוגה **User Access Settings** (הגדרות גישת משתמשים), מנהלי מערכת מציינים את הקבוצות או המשתמשים המורשים להשתמש בדפים Simple Configuration (תצורה פשוטה) ו-Device Class Configuration (תצורת מחלקות התקנים).

הערה: משתמשים או קבוצות זקוקים לזכויות מסוג Full User Administrator rights (זכויות מלאות של מנהל משתמשים) כדי לשנות את ההגדרה בתצוגה User Access Settings (הגדרות גישת משתמשים).

- יש להעניק למשתמש או לקבוצה גישה מסוג View (Read-only) Configuration Settings (הצגה (קריאה בלבד) של הגדרות תצורה) בתצוגה User Access Settings (הגדרות גישת משתמשים) כדי להציג את המידע בתצוגות Simple Configuration (תצורה פשוטה) ו-Device Class Configuration (תצורת מחלקות התקנים).
- יש להעניק למשתמש או לקבוצה גישה מסוג Change Configuration Settings (שינוי הגדרות תצורה) בתצוגה User Access Settings (הגדרות גישת משתמשים) כדי לשנות את המידע בתצוגות Simple Configuration (תצורה פשוטה) ו-Device Class Configuration (תצורת מחלקות התקנים).

הערה: גם חברים בקבוצה Administrators (מנהלי מערכת) חייבים לקבל גישת קריאה להצגת התצוגות Simple Configuration (תצורה פשוטה) ו-Device Class Configuration (תצורת מחלקות התקנים) וגישת שינוי לשינוי נתונים באמצעות אותן התצוגות.

הערה: לאחר ההערכה של רמות הגישה עבור כל המשתמשים והקבוצות, אם לא צוין Allow (אפשר) או Deny (חסום) ברמת גישה מסוימת עבור משתמש כלשהו, גישת המשתמש נחסמת באותה הרמה.

הענקת גישה לקבוצה או משתמש קיימים

כדי להעניק הרשאה לקבוצה או משתמש קיימים להציג או לשנות את הגדרות התצורה, בצע את השלבים הבאים:

1. בחלונית השמאלית או הימנית של **HP ProtectTools Administrative Console**, לחץ על **Device Access Manager** (מנהל הגישה להתקנים) ולאחר מכן לחץ על **User Access Settings** (הגדרות גישת משתמשים).
2. לחץ על קבוצה או משתמש כדי לאפשר להם גישה.
3. תחת **Permissions** (הרשאות), לחץ על **Allow** (אפשר) עבור כל סוג הרשאה שיש להעניק לקבוצה או למשתמש שנבחרו:

   הערה: ההרשאות המוענקות הן מצטברות. לדוגמה, משתמש שמקבל הרשאה מסוג Change Configuration Settings (שינוי הגדרות תצורה), מקבל באופן אוטומטי את ההרשאה View (Read-only) Configuration Settings (הצגה (קריאה בלבד) של הגדרות תצורה). משתמש שמקבל את ההרשאה Full User Administrator Rights (זכויות מלאות של מנהל משתמשים), מקבל גם את את ההרשאות Change Configuration Settings (שינוי הגדרות תצורה) ו-View (Read-only) Configuration Settings (הצגה (קריאה בלבד) של הגדרות תצורה).

   - Full User Administrator Rights (זכויות מלאות של מנהל משתמשים)
   - Change Configuration Settings (שינוי הגדרות תצורה)
   - View (Read-only) Configuration Settings (הצגה (קריאה בלבד) של הגדרות תצורה)
4. לחץ על הסמל **Save** (שמור).

חסימת גישה של קבוצה או משתמש קיימים

כדי למנוע מקבוצה או ממשתמש קיימים להציג או לשנות את הגדרות התצורה, בצע את השלבים הבאים:

1. בחלונית השמאלית או הימנית של **HP ProtectTools Administrative Console**, לחץ על **Device Access Manager** (מנהל הגישה להתקנים) ולאחר מכן לחץ על **User Access Settings** (הגדרות גישת משתמשים).
2. לחץ על קבוצה או משתמש שיש לחסום את גישתם.
3. תחת **Permissions** (הרשאות), לחץ על **Deny** (חסום) עבור כל סוג הרשאה שיש לחסום עבור הקבוצה או המשתמש שנבחרו:
   - Full User Administrator Rights (זכויות מלאות של מנהל משתמשים)
   - Change Configuration Settings (שינוי הגדרות תצורה)
   - View (Read-only) Configuration Settings (הצגה (קריאה בלבד) של הגדרות תצורה)
4. לחץ על הסמל **Save** (שמור).

הוספת קבוצה או משתמש חדשים

כדי להעניק גישה לקבוצה או משתמש חדשים להצגה או שינוי של הגדרות התצורה, בצע את השלבים הבאים:

1. בחלונית השמאלית או הימנית של **HP ProtectTools Administrative Console**, לחץ על **Device Access Manager** (מנהל הגישה להתקנים) ולאחר מכן לחץ על **User Access Settings** (הגדרות גישת משתמשים).
2. לחץ על **Add** (הוסף). תיבת הדו-שיח **Select Users or Groups** (בחירת משתמשים או קבוצות) נפתחת.
3. לחץ על **Advanced** (מתקדם) ולאחר מכן לחץ על **Find Now** (מצא כעת) כדי לחפש אחר משתמשים או קבוצות להוספה.
4. לחץ על קבוצה או משתמש, לחץ על **OK** (אישור) ולאחר מכן לחץ שוב על **OK**.
5. לחץ על **Allow** (אפשר) כדי להעניק גישת משתמש זו.
6. לחץ על הסמל **Save** (שמור).

הסרת גישה של קבוצה או משתמש

כדי להסיר הרשאה של קבוצה או משתמש להצגה או לשינוי של הגדרות התצורה, בצע את השלבים הבאים:

1. בחלונית השמאלית או הימנית של **HP ProtectTools Administrative Console**, לחץ על **Device Access Manager** (מנהל הגישה להתקנים) ולאחר מכן לחץ על **User Access Settings** (הגדרות גישת משתמשים).
2. לחץ על קבוצה או משתמש ולאחר מכן לחץ על **Remove** (הסר).
3. לחץ על הסמל **Save** (שמור).

תיעוד קשור

Device Access Manager for HP ProtectTools תואם למוצר הארגוני HP ProtectTools Enterprise Device Access Manager. בעת העבודה עם המוצר הארגוני, Device Access Manager for HP ProtectTools מאפשר גישת קריאה בלבד למאפיינים שלו.

מידע נוסף אודות Device Access Manager for HP ProtectTools זמין באינטרנט בכתובת http://www.hp.com/hps/security/products.

12 LoJack Pro for HP ProtectTools

קו מוצרי Computrace של Absolute Software מאפשר למשתמשים לעקוב אחר מחשבי ה-HP שלהם ולשפר את ההגנה על הנתונים. כמו-כן, מוצרי LoJack של Computrace מצמצמים את אובדן המחשבים ומסייעים בשחזור של מחשבים שנגנבו.

כדי להפעיל את מוצר Computrace, פעל בהתאם להוראות הבאות:

1. לחץ על **Start** (התחל), לחץ על **All Programs** (כל התוכניות), ולאחר מכן לחץ על **HP ProtectTools Security Manager**.
2. לחץ על **Theft Recovery** (שחזור מגניבה), ולאחר מכן לחץ על **Activate Now** (הפעל כעת).

דפדפן האינטרנט המוגדר כברירת מחדל פותח אתר אינטרנט לרישום שבו תוכל לבחור ולרכוש אחד משלושת מוצרי Computrace הזמינים עם HP ProtectTools:

- **Computrace Data Delete** (מחיקת נתוני Computrace)—כולל מחיקת נתונים מרוחקים, הקפאת התקן וכן מעקב ודיווח על נכסים בסיסיים.
- **Computrace LoJack Pro**—כולל מחיקת נתונים מרוחקים, הקפאת התקן, מעקב ודיווח על נכסים בסיסיים וכן שחזור מנוהל מגניבה.
- **Computrace LoJack Pro Premium**—כולל מחיקת נתונים מרוחקים, הקפאת התקן, מעקב ודיווח מתקדמים על נכסים, מיקום גיאוגרפי וגידור גיאוגרפי ושחזור מנוהל מגניבה.

Computrace Agent (סוכן Computrace) משובץ ב-BIOS של מחשבים ניידים עסקיים של HP, על אף שה-Agent (סוכן) מושבת בעת שליחת המחשב. לאחר רכישת המנוי, ניתן להפעיל את ה-Agent (סוכן). ה-Agent (סוכן) המשובץ יכול להתקין מחדש את מערכת ההפעלה ולאתחל מחדש כוננים קשיחים.

הערה: תקופות מינוי החל משנה ועד 5 שנים זמינות. עיין בהסכם המנוי של Absolute Software לקבלת פרטים נוספים. מאפיין השחזור תלוי במיקום הגיאוגרפי שלך. מעקב GPS נתמך בדגמים נבחרים עם התוספת WWAN.

13 פתרון בעיות

HP ProtectTools Security Manager

תיאור קצר	פרטים	פתרון
כרטיסים חכמים ואסימוני USB אינם זמינים ב-Security Manager (מנהל האבטחה) אם הותקנו לאחר ההתקנה של Security Manager.	כדי להשתמש בכרטיסים חכמים או באסימוני USB ב-Security Manager (מנהל האבטחה), התוכנה התומכת (מנהלי התקן, ספקי PKCS#11 וכולי) חייבת להיות מותקנת לפני ההתקנה של Security Manager. אם כבר התקנת את Security Manager (מנהל האבטחה), בצע את השלבים הבאים לאחר ההתקנה של התוכנה התומכת של הכרטיס החכם או האסימון:	היכנס ל-Password Manager (מנהל הסיסמאות). ב-HP ProtectTools Security Manager, לחץ על **Password Manager** (מנהל הסיסמאות), לחץ על **Credentials** (הרשאות) ולאחר מכן לחץ על **Smart Card** (כרטיס חכם). הפעל את המחשב מחדש, אם תתבקש לעשות זאת.
דפי אינטרנט מסוימים של יישומים יוצרים שגיאות שמונעות מהמשתמש לבצע או להשלים משימות.	יישומים מסוימים מבוססי-אינטרנט מפסיקים לפעול ומדווחים על שגיאות עקב הדפוס להשבתת פונקציונליות של Single Sign On (כניסה יחידה). לדוגמה, ניתן להבחין בסימן **!** בתוך משולש צהוב ב-Internet Explorer, המציין שאירעה שגיאה.	המאפיין Security Manager Single Sign On (כניסה יחידה) של מנהל האבטחה) אינו תומך בכל ממשקי האינטרנט של התוכנה. השבת תמיכת Single Sign On (כניסה יחידה) עבור דף האינטרנט הספציפי על-ידי ביטול התמיכה. עיין בתיעוד המלא אודות Single Sign On (כניסה יחידה), הזמין בקובצי עזרת התוכנה של Security Manager (מנהל האבטחה). אם לא ניתן להשבית Single Sign On (כניסה יחידה) ספציפית עבור יישום נתון, פנה לתמיכה הטכנית של HP ובקש תמיכה ברמה שלישית באמצעות איש הקשר שלך בשירות HP.
האפשרות **Browse for Virtual Token** (חיפוש אחר Token וירטואלי) אינה מוצגת במהלך הכניסה.	למשתמש אין אפשרות להעביר את המיקום של אסימון וירטואלי רשום ב-Password Manager (מנהל הסיסמאות) משום שאפשרות העיון הוסרה כדי לצמצם את סיכוני האבטחה.	אפשרות החיפוש הוסרה משום שהיא איפשרה לאנשים שאינם משתמשים למחוק קבצים או לשנות את שמותיהם ולהשתלט על Windows.
מנהלי מערכת של תחום אינם יכולים לשנות סיסמת Windows גם אם יש להם אישור לכך.	הבעיה מתרחשת לאחר שמנהל תחום נכנס לתחום ורושם את זהות התחום אצל Password Manager (מנהל הסיסמאות) באמצעות חשבון עם זכויות מנהל מערכת בתחום ובמחשב המקומי. כאשר מנהל התחום מנסה לשנות את סיסמת Windows מתוך Password Manager (מנהל הסיסמאות), מתקבלת כשל כניסה שגויה: **User account restriction** (הגבלת חשבון משתמש).	ל-Password Manager (מנהל הסיסמאות) אין אפשרות לשנות סיסמת חשבון של משתמש תחום באמצעות **Change Windows password** (שינוי סיסמת Windows). Security Manager (מנהל האבטחה) יכול לשנות רק את סיסמאות החשבון במחשב המקומי. משתמש התחום יכול לשנות את הסיסמה שלו באמצעות האפשרות **Change password** (שנה סיסמה) של **Windows security** (אבטחת Windows), אך משום שלמשתמש התחום אין חשבון פיזי במחשב המקומי, Password Manager (מנהל הסיסמאות) יכול לשנות רק את הסיסמה המשמשת לכניסה.
ל-Password Manager (מנהל הסיסמאות) יש בעיות תאימות עם GINA של סיסמת Corel WordPerfect 12.	אם המשתמש נכנס ל-Password Manager (מנהל הסיסמאות), יוצר מסמך ב-WordPerfect ושומר יחד עם הגנה באמצעות סיסמה, ל-Password Manager אין אפשרות לזהות, באופן ידני או אוטומטי, את ה-GINA של הסיסמה.	HP מפתחת פתרון עוקף עבור שיפור עתידי של המוצר.

תיאור קצר	פרטים	פתרון
Password Manager (מנהל הסיסמאות) אינו מזהה את הלחצן **Connect** (התחבר) על-גבי המסך.	אם ההרשאה של Single Sign On (כניסה יחידה) עבור Remote Desktop Connection (RDP) (חיבור לשולחן עבודה מרוחק) מוגדרת ל-**Connect** (התחבר), בעת הפעלה מחדש של Single Sign On (כניסה יחידה), הוא תמיד נכנס ל-**Save As** (שמירה בשם) במקום ל-**Connect** (התחבר).	HP מפתחת פתרון עוקף עבור שיפור עתידי של המוצר.
למשתמש אין אפשרות להיכנס ל-Password Manager לאחר המעבר ממצב Standby (המתנה) למצב Hibernation (מצב שינה) ב-Windows XP Service Pack 1 בלבד.	לאחר מתן אפשרות למערכת לעבור למצבי השינה, למנהל המערכת או למשתמש אין אפשרות להיכנס ל-Password Manager (מנהל הסיסמאות) ומסך הכניסה של Windows ממשיך להופיע ללא קשר להרשאת הכניסה שנבחרה (סיסמה, טביעת אצבע או כרטיס Java).	עדכן את Windows ל-Service Pack 2 באמצעות Windows Update. עיין במאמר 813301 במאגר המידע של Microsoft בכתובת http://www.microsoft.com לקבלת מידע נוסף אודות הסיבה לבעיה. כדי להיכנס, המשתמש חייב לבחור את Password Manager (מנהל הסיסמאות) ולהיכנס. לאחר הכניסה ל-Password Manager (מנהל הסיסמאות), המשתמש מתבקש להיכנס ל-Windows (ייתכן שהמשתמש יצטרך לבחור את אפשרות הכניסה ל-Windows) כדי להשלים את תהליך הכניסה. אם המשתמש נכנס קודם ל-Windows, עליו להיכנס ידנית ל-Password Manager (מנהל הסיסמאות).
תהליך **Restore Identity** (שחזור זהות) של האבטחה מאבד את השיוך ל-Token וירטואלי.	כאשר המשתמש משחזר זהות, Password Manager (מנהל הסיסמאות) עלול לאבד את השיוך למיקום האסימון הווירטואלי במסך הכניסה. למרות שהאסימון הווירטואלי רשום ב-Password Manager (מנהל הסיסמאות), המשתמש חייב לרשום את האסימון מחדש כדי לשחזר את השיוך.	נכון לעכשיו תופעה זו היא חלק מתכנון המוצר. בעת הסרת ההתקנה של Security Manager (מנהל האבטחה) ללא שמירת זהויות, חלק המערכת (השרת) של האסימון מושמד כך שלא ניתן עוד להשתמש באסימון לכניסה, גם אם חלק הלקוח של האסימון משוחזר באמצעות שחזור זהות. HP מפתחת אפשרויות לפתרון לטווח ארוך.

Device Access Manager for HP ProtectTools

גישת משתמשים להתקנים נחסמה בתוך Device Access Manager (מנהל הגישה להתקנים), אך ההתקנים עדיין נגישים.

- **הסבר** - נעשה שימוש ב-Simple Configuration (תצורה פשוטה) ו/או ב-Device Class Configuration (תצורת מחלקות התקנים) בתוך Device Access Manager (מנהל הגישה להתקנים) לחסימת גישת משתמשים להתקנים. למרות חסימת הגישה, למשתמשים עדיין יש גישה להתקנים.
- **פתרון:**
  - ודא ששירות HP ProtectTools Device Locking הופעל.
  - בתור משתמש ניהולי, לחץ על **Control Panel** (לוח הבקרה) ולאחר מכן לחץ על **System and Maintenance** (מערכת ותחזוקה). בחלון Administrative Tools (כלי ניהול), לחץ על **Services** (שירותים) וחפש את השירות **HP ProtectTools Device Locking/Auditing**. ודא שהשירות הופעל ושסוג האתחול הוא **Automatic** (אוטומטי).

למשתמש יש גישה לא צפויה להתקן או שגישתו להתקן נחסמה באופן לא צפוי.

- **הסבר** - Device Access Manager (מנהל הגישה להתקנים) שימש לחסימת גישת משתמשים להתקנים מסוימים ולמתן גישה למשתמשים להתקנים אחרים. בעת השימוש במערכת, למשתמש יש אפשרות לגשת להתקנים שלדעתו Device Access Manager (מנהל הגישה להתקנים) חסם את הגישה אליהם ולהיפך.
- **פתרון:**
  - השתמש ב-Device Class Configuration (תצורת מחלקות התקנים) ב-Device Access Manager (מנהל הגישה להתקנים) כדי לחקור את הגדרות ההתקנים של המשתמש.
  - לחץ על **Security Manager** (מנהל האבטחה), לחץ על **Device Access Manager** (מנהל הגישה להתקנים) ולאחר מכן לחץ על **Device Class Configuration** (תצורת מחלקות התקנים). הרחב את הרמות בעץ מחלקות ההתקנים וסקור את ההגדרות שחלות על משתמש זה. חפש הרשאות מסוג Deny (חסום) שייתכן שהוגדרו עבור המשתמש או קבוצת Windows שבה הוא חבר, למשל Users (משתמשים) או Administrators (מנהלי מערכת).

מתן אפשרות או חסימה, מי מקבל עדיפות?

- **הסבר** - ב-Device Class Configuration (תצורת מחלקות התקנים), מוגדרת התצורה הבאה:
  - ההרשאה Allow (אפשר) הוענקה לקבוצת Windows (למשל, BUILTIN\Administrators) וההרשאה Deny (חסום) הוענקה לקבוצת Windows אחרת (למשל, BUILTIN\Users) באותה רמה בהיררכיית מחלקת ההתקנים (למשל, כונני DVD/CD).
  - אם משתמש כלשהו חבר בשתי הקבוצות (כגון מנהל מערכת), מי מהן מקבלת עדיפות?
- **פתרון:**
  - גישת המשתמש להתקן נחסמת. חסימה עדיפה על מתן אפשרות.
  - הגישה נחסמת בשל הדרך שבה Windows מברר את ההרשאה הישימה עבור ההתקן. קבוצה אחת נחסמת וקבוצה אחת מקבלת גישה, אך המשתמש חבר בשתי הקבוצות. המשתמש נחסם משום שחסימת גישה מקבלת עדיפות על-פני מתן גישה.
  - פתרון עוקף אחד לכך הוא לחסום את הגישה של קבוצת Users (משתמשים) ברמה DVD/CD-ROM Drives (כונני CD/DVD) ולהתיר את הגישה של קבוצת Administrators (מנהלי מערכת) ברמה שמתחת ל-DVD/CD-ROM Drives.
  - פתרון עוקף חלופי הוא יצירת קבוצות Windows ספציפיות, האחת למתן גישה ל-DVD/CD והאחרת לחסימת הגישה להתקנים אלה. לאחר מכן, ניתן יהיה להוסיף משתמשים ספציפיים לקבוצה המתאימה.

התצוגה Simple Configuration (תצורה פשוטה) שימשה להגדרת מדיניות בקרת גישה להתקנים, אך משתמשים ניהוליים לא מסוגלים לגשת להתקנים.

- **הסבר** - Simple Configuration (תצורה פשוטה) חוסמת גישה של משתמשים ואורחים ומאפשרת גישה של מנהלי התקנים.
- **פתרון:** הוסף את המשתמש הניהולי לקבוצה Device Administrators (מנהלי התקנים).

שונות

תופעות הקשורות לתוכנה - תיאור קצר	פרטים	פתרון
Security Manager (מנהל האבטחה) - מתקבלת האזהרה: **The security application can not be installed until the HP Protect Tools Security Manager is installed.** (לא ניתן להתקין את יישום האבטחה לפני שיותקן HP Protect Tools Security Manager.)	כל יישומי האבטחה, כגון Java Card Security (אבטחת כרטיס Java) וקוראים ביומטריים, הם יישומי Plug-in הניתנים להרחבה עבור ממשק Security Manager (מנהל האבטחה). יש להתקין את Security Manager (מנהל האבטחה) לפני שניתן יהיה לטעון יישום Plug-in של אבטחה המאושר על-ידי HP.	יש להתקין את תוכנת Security Manager לפני התקנה של Plug-in אבטחה כלשהו.
HP ProtectTools Security Manager - לסירוגין, שגיאה חוזרת במהלך סגירה של ממשק ה-Security Manager (מנהל האבטחה).	לסירוגין (מקרה אחד מ-12), שגיאה נוצרת על-ידי שימוש בלחצן הסגירה בפינה הימנית או השמאלית העליונה של המסך לצורך סגירה של ה-Security Manager (מנהל האבטחה) לפני שכל יישומי ה-Plug-in סיימו להיטען.	הדבר קשור לתלות בתזמון בזמני הטעינה של שירותי Plug-in בעת סגירה והפעלה מחדש של ה-Security Manager (מנהל האבטחה). מכיוון ש-PTHOST.exe הוא המעטפת שמאכלסת את היישומים האחרים (יישומי Plug-in), הוא תלוי ביכולת ה-Plug-in להשלים את זמן הטעינה שלו (שירותים). סגירת המעטפת לפני שה-Plug-in השלים את הטעינה היא הגורם לבעיה. אפשר ל-Security Manager (מנהל האבטחה) להשלים את ההודעה של טעינת השירותים (המוצגת בחלקו העליון של חלון ה-Security Manager) וכל יישומי ה-Plug-in המפורטים בעמודה השמאלית. למניעת כשל, הקצה פרק זמן סביר לטעינה של יישומי Plug-in אלה.
HP ProtectTools - גישה לא מוגבלת או זכויות מנהל מערכת לא מבוקרות מהוות סכנה.	סיכונים רבים מתאפשרים כאשר ניתנת גישה לא מוגבלת למחשב הלקוח, לרבות הסיכונים הבאים: ● מחיקת ה-PSD ● שינוי זדוני של הגדרות משתמש ● השבתה של פונקציות ומדיניות הקשורות לאבטחה	המנהלים מוזמנים להשתמש בשיטות העבודה המומלצות בהגבלת הרשאות של משתמשי קצה ובהגבלת גישת משתמשים. אין להעניק למשתמשים לא מורשים הרשאות של מנהל המערכת.

מילון מונחים

ATM Automatic Technology Manager (מנהל טכנולוגיות אוטומטי), המאפשר למנהלי רשתות לנהל מערכות מרחוק ברמת ה-BIOS.

Drive Encryption (הצפנת כונן) המאפיין מגן על הנתונים על-ידי הצפנת הכוננים הקשיחים והפיכת המידע לבלתי קריא לאנשים ללא הרשאה מתאימה.

DriveLock מאפיין אבטחה המקשר את הכונן הקשיח למשתמש ודורש מהמשתמש להקליד את הסיסמה הנכונה של DriveLock כאשר המחשב מופעל.

Encryption File System (EFS) (מערכת הצפנת קבצים) מערכת המצפינה את כל הקבצים ותיקיות המשנה בתוך התיקייה הנבחרת.

HP SpareKey עותק גיבוי של מפתח הצפנת כונן.

Java Card כרטיס שניתן להסרה המוכנס למחשב. הוא מכיל פרטי זיהוי לצורך כניסה. על מנת לבצע כניסה בעזרת כרטיס Java Card במסך הכניסה של Drive Encryption (הצפנת כונן) עליך להכניס כרטיס Java Card ולהקליד את שם המשתמש ומספר הזיהוי האישי (PIN) של כרטיס Java Card.

Live Messenger History Viewer רכיב של Privacy Manager Chat (צ'אט של מנהל פרטיות) המאפשר לך לחפש אחר שיחות מוצפנות בהיסטוריית הצ'אט ולהציג אותן.

PIN (מספר זיהוי אישי) מספר זיהוי אישי.

PKI תקן של Public Key Infrastructure (תשתית מפתחות ציבורית) המגדיר את הממשקים ליצירה, שימוש וניהול של אישורים ומפתחות קריפטוגרפיים.

PSD כונן מאובטח אישי המספק אזור אחסון מוגן למידע רגיש.

Single Sign On (כניסה יחידה) מאפיין המאחסן מידע אימות ומאפשר לך להשתמש ב-Security Manager (מנהל האבטחה) כדי לגשת לאינטרנט וליישומי Windows הדורשים אימות סיסמה.

Token ראה 'שיטת כניסה מאובטחת'.

Token וירטואלי מאפיין אבטחה הפועל באופן דומה לכרטיס Java Card וקורא כרטיסים. ה-Token נשמר בכונן הקשיח של המחשב או ברישום של Windows. כאשר אתה מבצע כניסה באמצעות Token וירטואלי, אתה מתבקש להזין מספר זיהוי אישי (PIN) של משתמש כדי להשלים את האימות.

Token מסוג USB התקן אבטחה המאחסן פרטי זיהוי אודות משתמש. בדומה לכרטיס Java Card או קורא ביומטרי, הוא משמש לאימות הבעלים של המחשב.

Trusted Contact (איש קשר מהימן) אדם שקיבל הזמנה ל-Trusted Contact (איש קשר מהימן).

TXT Trusted Execution Technology (טכנולוגיית הפעלה מהימנה).

Windows Logon Security (אבטחת כניסה של Windows) מאפיין שמגן על חשבונות Windows על-ידי דרישת שימוש בהרשאות ספציפיות לקבלת גישה.

אימות תהליך של אימות הרשאת משתמש לביצוע משימה כגון גישה למחשב, שינוי הגדרות עבור תוכנית מסוימת או הצגה של נתונים מאובטחים.

אימות במהלך הפעלה מאפיין אבטחה הדורש סוג מסוים של אימות, כגון כרטיס Java Card, שבב אבטחה או סיסמה, כאשר המחשב מופעל.

אישור דיגיטלי הרשאות אלקטרוניות המאשרות את זהותם של אדם או חברה באמצעות כבילת הזהות של בעל האישור הדיגיטלי לזוג מפתחות אלקטרוניים המשמשים לחתימה על מידע דיגיטלי.

אישור של Privacy Manager (מנהל הפרטיות) אישור דיגיטלי הדורש אימות בכל פעם שאתה משתמש בו לצורך ביצוע פעולות קריפטוגרפיות, כגון חתימה והצפנה של הודעות דואר אלקטרוני ומסמכים של Microsoft Office.

ארכיון שחזור חירום אזור אחסון מוגן המאפשר הצפנה מחדש של מפתחות המשתמש הבסיסיים ממפתח של בעל פלטפורמה אחד לאחר.

אתחול תהליך הפעלה מחדש של המחשב.

ביומטרי קטגוריה של הרשאות אימות המשתמשות במאפיין פיזי, כגון טביעת אצבע, לצורך זיהוי המשתמש.

גיבוי השתמש במאפיין הגיבוי לשמירת עותק של מידע חשוב של תוכנית במיקום מחוץ לתוכנית. לאחר מכן, ניתן להשתמש במאפיין לשחזור המידע בשלב מאוחר יותר באותו המחשב או במחשב אחר.

גילוי משימה המאפשרת למשתמש לפענח שיחה אחת או יותר מתוך היסטוריית הצ'אט, תוך הצגת ה-Contact Screen Name (שם המסך של איש הקשר) כטקסט רגיל והפיכת השיחה לזמינה לצורך הצגה.

גריסה הפעלה של אלגוריתם שיוצר ערפול של הנתונים שבתוך הנכס.

גריסה אוטומטית גריסה מתוזמנת שהמשתמש מגדיר ב-File Sanitizer (מנקה הקבצים).

גריסה ידנית גריסה מיידית של נכס או נכסים נבחרים, העוקפת את תזמון הגריסה האוטומטי.

הודעה מהימנה התקשרות שבמהלכה הודעות מהימנות נשלחות משולח מהימן ל-Trusted Contact (איש קשר מהימן).

הזמנה ל-Trusted Contact (איש קשר מהימן) דואר אלקטרוני שנשלח לאדם, המבקש ממנו להפוך ל-Trusted Contact (איש קשר מהימן).

הלבנת שטח פנוי כתיבה מאובטחת של נתונים אקראיים על-גבי נכסים שנמחקו כדי לעוות את התוכן של הנכס שנמחק.

העברה משימה המאפשרת ניהול, שחזור והעברה של Privacy Manager Certificates (אישורים של מנהל הפרטיות) ו-Trusted Contacts (אנשי קשר מהימנים).

הפעלה המשימה שיש לבצע לפני שניתן לגשת לכל מאפיין שהוא ב-Drive Encryption (הצפנת כונן). המאפיין Drive Encryption (הצפנת כונן) מופעל באמצעות אשף ההתקנה של HP ProtectTools. רק מנהל מערכת יכול להפעיל את Drive Encryption (הצפנת כונן). תהליך ההפעלה כולל הפעלה של התוכנה, הצפנה של הכונן, יצירת חשבון משתמש ויצירת מפתח ההצפנה עבור הגיבוי ההתחלתי על-גבי התקן אחסון נשלף.

הפעלת היסטוריית צ'אט קובץ מוצפן המכיל תיעוד של שני הצדדים בשיחה במהלך צ'אט.

הצפנה הליך, כגון שימוש באלגוריתם, המשמש בקריפטוגרפיה לצורך המרה של טקסט רגיל לטקסט מוצפן במטרה למנוע מנמענים לא מורשים לקרוא נתונים אלה. ישנם סוגים רבים של הצפנת נתונים והם מהווים בסיס לאבטחת רשת. סוגים נפוצים כוללים את Data Encryption Standard (תקן הצפנת נתונים) והצפנה של מפתח ציבורי.

הרשאות שיטה שלפיה משתמש מוכיח שהוא מורשה לבצע משימה מסוימת בתהליך האימות.

זהות ב-HP ProtectTools Security Manager, קבוצה של הרשאות והגדרות המנוהלת כמו חשבון או פרופיל עבור משתמש מסוים.

חותם מוצע משתמש הממונה על-ידי הבעלים של מסמך ב-Microsoft Word או Microsoft Excel להוסיף שורת חתימה למסמך.

חותם עבור אנשי קשר מהימנים משימה המוסיפה חתימה דיגיטלית, מצפינה את הדואר האלקטרוני ושולחת אותו לאחר שביצעת אימות באמצעות שיטת הכניסה המאובטחת שבחרת.

חשבון משתמש של Windows פרופיל עבור אדם המורשה להתחבר לרשת או למחשב נפרד.

חשבון רשת חשבון של משתמש או מנהל מערכת ב-Windows, במחשב מקומי, בקבוצת עבודה או בתחום.

חתימה דיגיטלית נתונים הנשלחים יחד עם קובץ המאמתים את זהותו של האדם השולח את החומר, ומוודאים שלא בוצעו שינויים בקובץ לאחר שנחתם.

טביעת אצבע דימוי דיגיטלי של תמונת טביעת אצבע. תמונת טביעת האצבע הממשית לעולם אינה מאוחסנת ב-Security Manager (מנהל האבטחה).

כניסה אובייקט ב-Security Manager (מנהל האבטחה) המורכב משם משתמש וסיסמה (ייתכן שבנוסף למידע אחר שנבחר) שיכול לשמש לכניסה לאתרי אינטרנט או תוכניות אחרות.

כרטיס זיהוי אביזר של הסרגל הצידי של Windows אשר משמש לזיהוי חזותי של שולחן העבודה שלך באמצעות שם המשתמש שלך ותמונה שבחרת. לחץ על כרטיס הזיהוי כדי לפתוח את HP ProtectTools Administrative Console.

כרטיס חכם רכיב חומרה קטן, דומה בגודלו ובצורתו לכרטיס אשראי, המאחסן פרטי זיהוי של בעל הכרטיס. משמש לאימות בעל הכרטיס במחשב.

לוח מחוונים מקום מרכזי שממנו ניתן לגשת ולנהל את המאפיינים ואת ההגדרות ב-Security Manager (מנהל האבטחה) עבור HP ProtectTools.

לחצן Send Security (אבטחת שליחה) לחצן תוכנה המוצג בסרגל הכלים של הודעות הדואר האלקטרוני ב-Microsoft Outlook. לחיצה על הלחצן מאפשרת לך לחתום ו/או להצפין הודעת דואר אלקטרוני של Microsoft Outlook.

לחצן Sign and Encrypt (חתום והצפן) לחצן תוכנה המוצג בסרגל הכלים של יישומי Microsoft Office. לחיצה על הלחצן מאפשרת לך לחתום, להצפין או להסיר הצפנה במסמך של Microsoft Office.

מדיניות בקרת גישה להתקנים רשימת ההתקנים שהגישה אליהם מותרת או חסומה.

מחזור גריסה מספר הפעמים שבהן אלגוריתם הגריסה מופעל בכל נכס. ככל שמספר מחזורי הגריסה שתבחר יהיה גבוה יותר, כך המחשב יהיה מאובטח יותר.

מחיקה פשוטה מחיקה של התייחסות לנכס ב-Windows. תוכן הנכס נשאר בכונן הקשיח עד שנתונים מערפלים נכתבים על-גביו באמצעות הלבנה של שטח פנוי.

מחלקת התקנים כל ההתקנים מסוג מסוים, כגון כוננים.

מנהל מערכת *ראה* 'מנהל מערכת של Windows'.

מנהל מערכת של Windows משתמש בעל זכויות מלאות לשינוי הרשאות ולניהול משתמשים אחרים.

מסוף מקום מרכזי שממנו ניתן לגשת ולנהל את המאפיינים ואת ההגדרות ב-HP ProtectTools Administrative Console.

מסך כניסה של Drive Encryption (הצפנת כונן) מסך כניסה המוצג לפני ש-Windows מופעל. על המשתמשים להזין את שם המשתמש והסיסמה שלהם ב-Windows או את מספר הזיהוי האישי (PIN) של כרטיס Java Card שברשותם. ברוב המקרים, הזנת הפרטים הנכונים במסך הכניסה של Drive Encryption (הצפנת כונן) מאפשרת גישה ישירה ל-Windows ללא צורך לבצע כניסה שנית במסך הכניסה של Windows.

מצב התקן SATA מצב העברת נתונים בין המחשב לבין התקני אחסון גדולים, כגון כוננים קשיחים וכוננים אופטיים.

משתמש כל אדם שרשום ב-Drive Encryption (הצפנת כונן). למשתמשים שאינם מנהל מערכת יש זכויות מוגבלות ב-Drive Encryption (הצפנת כונן). הם יכולים להירשם (באישור מנהל המערכת) ולהיכנס בלבד.

משתמש מורשה משתמש שקיבל הרשאה בתצוגה User Access Settings (הגדרות גישת משתמשים) להציג או לשנות הגדרות תצורה בתצוגות Simple Configuration (תצורה פשוטה) או Device Class Configuration (תצורת מחלקות התקנים).

נכס רכיב נתונים המורכב ממידע פרטי או קבצים, נתונים היסטוריים או נתונים הקשורים לאינטרנט וכו', הממוקם בכונן הקשיח.

נמען של Trusted Contact (איש קשר מהימן) אדם המקבל הזמנה להפוך ל-Trusted Contact (איש קשר מהימן).

סיסמת ביטול סיסמה שנוצרת כאשר משתמש מבקש אישור דיגיטלי. הסיסמה דרושה כאשר משתמש רוצה לבטל את האישור הדיגיטלי שלו. הדבר מבטיח שרק המשתמש יוכל לבטל את האישור.

סמכות אישור שירות שמנפיק את האישורים הדרושים להפעלה של תשתית מפתחות ציבורית.

ספק שירות קריפטוגרפיה (CSP) ספק או ספרייה של אלגוריתמים קריפטוגרפיים שניתן להשתמש בהם בממשק מוגדר היטב לצורך ביצוע פונקציות קריפטוגרפיות מסוימות.

סצינה צילום של משתמש רשום המשמש לאימות.

פרופיל גריסה שיטת מחיקה מסוימת ורשימת נכסים.

קבוצה קבוצת משתמשים בעלי אותה רמת גישה או חסימה למחלקת התקנים או התקן ספציפי.

קריפטוגרפיה שימוש בנתוני הצפנה ופענוח באופן שבו רק אנשים מסוימים יכולים לפענח אותם.

רצף מקשים שילוב של מקשים מסוימים אשר בעת לחיצה עליהם יוזם גריסה אוטומטית - לדוגמה, s+alt+ctrl.

רשימת Trusted Contact (איש קשר מהימן) רשימה של אנשי קשר מהימנים.

שולח מהימן איש קשר מהימן השולח הודעות דואר אלקטרוני ומסמכים של Microsoft Office שנחתמו ו/או הוצפנו.

שורת חתימה שדה המיועד לתצוגה החזותית של חתימה דיגיטלית. כאשר מסמך נחתם, שמו של החותם ושיטת האימות מוצגים. כמו כן, ניתן לכלול את תאריך החתימה ואת תפקידו של החותם.

שחזור תהליך המעתיק מידע של תוכנית מקובץ גיבוי שנשמר בעבר לתוך תוכנית זו.

שיטת כניסה מאובטחת השיטה המשמשת לצורך כניסה למחשב.

שירות ברקע השירות ברקע HP ProtectTools Device Locking/Auditing, שחייב לפעול כדי להחיל מדיניות בקרת גישה להתקנים. ניתן להציגו מתוך היישום Services (שירותים) תחת האפשרות Administrative Tools (כלי ניהול) בלוח הבקרה. אם הוא אינו פועל, HP ProtectTools Security Manager מנסה להפעילו בעת החלה של מדיניות בקרת גישה להתקנים.

תחום קבוצה של מחשבים המהווים חלק מרשת וחולקים מסד נתונים משותף של ספריות. לכל תחום שם ייחודי משלו, וכל תחום כולל סדרה של כללים והליכים משותפים.

תיאור הליך שנעשה בו שימוש בקריפטוגרפיה כדי להמיר נתונים מוצפנים לטקסט רגיל.

תקשורת הודעות מיידיות (IM) מהימנה התקשורת שבמהלכה הודעות מהימנות נשלחות משולח מהימן ל-Trusted Contact (איש קשר מהימן).

אינדקס

א
אבטחה
מטרות מרכזיות 3
סיכום 36
תפקידים 5
אימות 13
איפוס 79
אישור, מוקצה מראש 45
אישור Privacy Manager (מנהל הפרטיות)
ביטול 47
בקשה 45
הגדרת ברירת מחדל 46
הצגת פרטים 46
התקנה 45
חידוש 46
מחיקה 46
קבלה 45
שחזור 47
אישור דיגיטלי
ביטול 47
בקשה 45
הגדרת ברירת מחדל 46
הצגת פרטים 46
התקנה 45
חידוש 46
מחיקה 46
קבלה 45
שחזור 47
אנשי קשר מהימנים
בדיקת מצב ביטול 50
הוספה 48
הצגת פרטים 49
מחיקה 49
אשף
התקנת HP ProtectTools 7
אשף התקנה 7

ב
בחירה
נכסים לגריסה 68
פרופיל גריסה 68
ביטול פעולת גריסה או הלבנה 72
בקרת גישה להתקנים 73
בקשת אישור דיגיטלי 45

ג
גיבוי
אישורי Privacy Manager (מנהל הפרטיות) 62
אנשי קשר מהימנים 62
הרשאות HP ProtectTools 6
נתונים 35
גישה
בקרה 73
הענקה לקבוצות או משתמשים
קיימים 80
חסימה 77
חסימה של קבוצות או משתמשים
קיימים 81
מניעה של גישה לא מורשית 3
מתן 77
גישה לא מורשית, מניעה 3
גניבה, הגנה מפני 3
גריסה ידנית
כל הפריטים שנבחרו 71
נכס אחד 71

ד
דרישות מערכת 43

ה
הגבלה
גישה להתקנים 73
גישה לנתונים רגישים 3
הגדרה
לוח זמנים לגריסה 67
לוח זמנים להלבנת שטח פנוי 67
נכסים לאישור לפני הגריסה 69
נכסים לאישור לפני המחיקה 69
הגדרות
הוספה 20, 25, 36
הכרטיסייה General (כללי) 19
יישומים 20, 25, 36
משתמש מתקדם 27
מתקדמות 17
סמל 32
הגדרות הכרטיסייה Applications (יישומים) 20, 36
הגדרות התקן
טביעת אצבע 16
כרטיס חכם 16
פנים 16
ציון 16
הגדרות לוח מחוונים 25
הגדרת תצורה
HP ProtectTools Administrative Console 12
Privacy Manager (מנהל הפרטיות) עבור Microsoft Outlook 51
Privacy Manager (מנהל הפרטיות) עבור Windows Live Messenger 57
Privacy Manager (מנהל הפרטיות) עבור מסמך Microsoft Office 53
איפוס 79
בקרת גישה 80
גישה להתקנים 74
הגדרות 80
יישומים 18
מחלקת התקנים 76
הגנה על נכסים מפני גריסה אוטומטית 69
הודעת דואר אלקטרוני
הוספת חותם עבור אנשי קשר מהימנים 52

הצגת הודעה עם חותם 52
חתימה 51
הוספה
חותמים מוצעים 53
משתמש 81
קבוצה 81
שורת חתימה 53
שורת חתימה של חותם מוצע 54
הוספת חותם 52
הוצאת נכסים ממחיקה אוטומטית 69
היסטוריית צ'אטים, הצגה 58
הכרטיסייה General (כללי),
הגדרות 19
הלבנת שטח פנוי 67
הסרה
גישת משתמש 81
גישת קבוצה 81
הצפנה ממסמך Microsoft
Office 55
העדפות, הגדרה 34
הפעלה
Drive Encryption (הצפנת
כונן) 39
הלבנת שטח פנוי 72
הצגה
הודעת דואר אלקטרוני עם
חותם 52
היסטוריית צ'אטים 58
מסמך חתום של Microsoft
Office 55
מסמך מוצפן של Microsoft
Office 56
קובצי יומן 72
הצפנה
כוננים 37, 40, 41
מסמך Microsoft Office 54
הרשאות 33, 34
הרשאות, רישום 26
השבתת Drive Encryption (הצפנת
כונן) 39
התאמה אישית
פרופיל גריסה 68
פרופיל מחיקה פשוטה 69
התחלת הפעלת צ'אט של Privacy
Manager (מנהל הפרטיות) 56
התקן, מתן גישה למשתמש 79

ח
חותם מוצע
הוספה 53
הוספת שורת חתימה 54
חסימת גישה 77
חתימה
הודעת דואר אלקטרוני 51
מסמך Microsoft Office 53

ט
טביעות אצבע
הגדרות 16
רישום 26

י
יישומים, הגדרת תצורה 18
יצירה
מפתחות גיבוי 41
פרופיל גריסה 68

כ
כלים, הוספה 21
כלי ניהול, הוספה 21
כניסה למחשב 39
כרטיסי זיהוי 34
כרטיסי חכם
הגדרות 16

מ
מאפייני HP ProtectTools 2
מאפיינים, HP ProtectTools 2
מחזור גריסה 68
מחיקה פשוטה 69
מחלקת התקנים
הגדרת תצורה 76
מתן גישה למשתמש 78
מטרות, אבטחה 3
מטרות אבטחה מרכזיות 3
מפתחות גיבוי, יצירה 41
מצב הצפנה, הצגה 40
מצב יישומי אבטחה 36
משתמש
הסרה 78
חסימת גישה 77
מתן גישה 77
מתן גישה 77

נ
ניהול
הרשאות 33
משתמשים 15
סיסמאות 20, 29
ניהול מרכזי 63
ניהול צ'אטים בחלון התקשרות 57
נתונים
גיבוי 35
הגבלת גישה אל 3
שחזור 35

ס
סיסמה
HP ProtectTools 5
הנחיות 6
מאובטחת 6
ניהול 5
עוצמה 32
קווי המדיניות 4
שינוי 27
סיסמת כניסה של Windows 5
סצינה
רישום 26

ע
עדכונים והודעות 22, 36

פ
פנים
הגדרות 16
רישום סצינות 26
פענוח כוננים 37, 41
פרופיל גריסה מוגדר מראש 68
פרטי כניסה
הוספה 30
ניהול 32
עריכה 31
קטגוריות 31
פתיחה
Device Access Manager for HP
ProtectTools 74
Drive Encryption for HP
ProtectTools 38
File Sanitizer for HP
ProtectTools 67
HP ProtectTools Administrative
Console 10
HP ProtectTools Security
Manager 24
Privacy Manager for HP
ProtectTools 44

פתרון בעיות
Device Access Manager (מנהל הגישה להתקנים) 85
Security Manager (מנהל האבטחה) 83
שונות 87

צ

ציון הגדרת אבטחה 14

ק

קבוצה
הסרה 78
חסימת גישה 77
מתן גישה 77
קביעת תצורה
פשוטה 74

ר

רישום
טביעות אצבע 26
סצינות 26
רישום הרשאות 26
רצף מקשים 70

ש

שחזור
אישורים ואנשי קשר מהימנים של Privacy Manager (מנהל הפרטיות) 62
הרשאות HP ProtectTools 6
נתונים 35
שחזור, ביצוע 42
שימוש
HP ProtectTools Administrative Console 11
שירות ברקע 75
שליחת מסמך מוצפן של Microsoft Office בדואר אלקטרוני 55

ת

תפקידי אבטחה 5

D

Device Access Manager for HP ProtectTools 73
Device Access Manager for HP ProtectTools
פתיחה 74
פתרון בעיות 85
Discover more (גלה עוד) 36
Drive Encryption for HP ProtectTools
הצפנת כוננים בודדים 41
ניהול Drive Encryption (הצפנת כונן) 41
פענוח כוננים בודדים 41
פתיחה 38
Drive Encryption for HP ProtectTools
גיבוי ושחזור 41
הפעלה 39
השבתה 39
כניסה לאחר הפעלת Drive Encryption (הצפנת כונן) 39

E

Excel, הוספת שורת חתימה 53

F

File Sanitizer for HP ProtectTools
הליכי הגדרה 67
סמל 71
פתיחה 67

H

HP ProtectTools Administrative Console
הגדרת תצורה 12
פתיחה 10
שימוש 11
HP ProtectTools Security Manager
הליכי הגדרה 26
סיסמת הגיבוי והשחזור 5
פתיחה 24
פתרון בעיות 83

J

Java Card Security for HP ProtectTools, PIN 5

L

Logons (פרטי כניסה)
תפריט 31
LoJack Pro 82

M

Microsoft Excel, הוספת שורת חתימה 53
Microsoft Office
הסרת הצפנה 55
הצגת מסמך חתום 55
הצגת מסמך מוצפן 56
הצפנת מסמך 54
חתימה על מסמך 53
שליחת מסמך מוצפן בדואר אלקטרוני 55
Microsoft Word, הוספת שורת חתימה 53

P

Password Manager 29
Password Manager (מנהל הסיסמאות) 29
Privacy Manager (מנהל הפרטיות)
שימוש ב-Windows Live Messenger 56
שימוש עם Microsoft Outlook 51
שימוש עם מסמך של Microsoft Office 2007 52
Privacy Manager for HP ProtectTools
הליכי הגדרה 44
העברת Privacy Manager Certificates (אישורים של מנהל הפרטיות) ו-Trusted Contacts (אנשי קשר מהימנים) למחשב אחר 62
Privacy Manager for HP ProtectTools
אישור Privacy Manager (מנהל הפרטיות) 44
דרישות מערכת 43
ניהול אישורים של Privacy Manager (מנהל הפרטיות) 44
ניהול אנשי קשר מהימנים 47
פתיחה 44
שיטות אימות 43
שיטות כניסה מאובטחת 43

S

Simple Configuration (תצורה פשוטה) 74

W

Windows Live Messenger, ניהול צ'אטים 57
Word, הוספת שורת חתימה 53