

המדריך לניהול מחשב שולחני מחשבים עסקיים

© Copyright 2008 Hewlett-Packard
Development Company, L.P.
בזאת נתון לשינויים ללא הודעה מראש.

הם Microsoft, Windows ו-Windows Vista סימנים מסחריים או סימנים מסחריים רשומים של
Microsoft Corporation בארצות הברית ו/או
במדינות/אזורים אחרים.

Intel ו-Pro v הם סימנים מסחריים של חברת Intel
Corporation בארה"ב ובמדינות אחרות.

כתבי האחריות היחידים החלים על מוצרים
ושירותים של HP מפורטים במפורש בהצהרות
האחריות הנלוות לאותם מוצרים ושירותים. אין
להבין מתוך הכתוב לעיל כי תחול על המוצר אחריות
נוספת כלשהי. חברת HP לא תישא בכל אחריות
שהיא לשגיאות טכניות או לשגיאות עריכה או
להשמטות במסמך זה.

מסמך זה מכיל נתוני בעלות המעוגנים בזכויות
יוצרים. אין להעתיק, לשכפל או לתרגם לשפה
אחרת חלקים כלשהם ממסמך זה ללא אישור
מראש ובכתב מחברת Hewlett Packard.

המדריך לניהול מחשב שולחני

מחשבים עסקיים

מהדורה שלישית (יולי 2008)

מק"ט מסמך: 451272-BB3

מדריך זה מספק הגדרות והראות לשימוש במאפייני האבטחה והניהול שהותקנו מראש בדגמים אחדים.

אזהרה! ⚠ טקסט המופיע בצורה זו מציין כי אי מילוי הוראות אלה עלול לגרום לנזק גופני חמור, ואף לגרום למוות.

זהירות: ⚠ טקסט המופיע בצורה זו מציין כי אי מילוי הוראות אלה עלול לגרום נזק לציוד, וכן לאובדן נתונים או מידע.

הערה: 📝 טקסט המופיע בצורה זו מספק מידע משלים חשוב.

תוכן העניינים

1 סקירה כללית של ניהול מחשב שולחני

2 הגדרת תצורה ראשונית ופריסה

3	HP Software Agent
3	Altiris Deployment Solution Agent

3 Remote System Installation (התקנת מערכת מרחוק)

4 עדכון וניהול תוכנות

5	HP Client Management Interface
6	HP SoftPaq Download Manager
7	HP System Software Manager
7	HP ProtectTools Security Manager
8	HP Client Automation מהדורות Starter ו-Standard
8	HP Client Automation Enterprise Edition
9	HP Client Manager מ-Symantec
10	ערכת Altiris Client Management Suite
10	HP Client Catalog עבור מוצרי Microsoft System Center ו-SMS
11	HP Backup and Recovery Manager (מנהל הגיבוי והשחזור של HP)
12	טכנולוגיית ניהול
14	Verdiem Surveyor
14	HP Proactive Change Notification
14	Subscriber's Choice
14	פתרונות שאינם בשימוש

5 זיכרון הבזק ROM

15	זיכרון הבזק Remote ROM Flash
15	HPQFlash

6 Boot Block Emergency Recovery Mode (מצב שחזור חירום של בלוק אתחול)

7 שכפול ההגדרות

17	העתקה למחשב אחד
----	-----------------

18	העתקה למספר מחשבים
18	יצירת התקן שניתן לאתחול
18	התקני USB flash media נתמכים
20	התקן USB flash media שאינו נתמך

8 לחצן הפעלה דו-מצבי

9 תמיכה באתר HP

10 סטנדרטים מקובלים בשוק

11 בקרת נכסים ואבטחה

28	אבטחה באמצעות סיסמה
28	קביעת סיסמת הגדרות באמצעות Computer Setup (הגדרות המחשב)
29	קביעת סיסמת הפעלה (Power-On) באמצעות Computer Setup (הגדרות המחשב)
29	הזנת סיסמת הפעלה
29	הזנת סיסמת הגדרות
30	שינוי סיסמת הפעלה או סיסמת הגדרות
30	מחיקת סיסמת הפעלה או סיסמת הגדרות
31	תווי הפרדה במקלדות של שפות שונות
31	ביטול סיסמאות
31	DriveLock
32	שימוש ב- DriveLock
32	יישומי DriveLock
33	Smart Cover Sensor (חיישן הכיסוי החכם)
33	הגדרת רמת ההגנה של ה-Smart Cover Sensor (חיישן הכיסוי החכם)
33	Smart Cover Lock (מנעול הכיסוי החכם)
34	נעילת מנעול הכיסוי החכם
34	שחרור מנעול הכיסוי החכם
34	שימוש ב-Smart Cover FailSafe Key
35	Cable Lock Provision (התקן מנעול כבל)
35	טכנולוגיה לזיהוי טביעות אצבע
35	הודעות כשל והתאוששות
35	Drive Protection System (מערכת להגנה על כוננים)
35	אספקת מתח עמידה בנחשולי מתח
35	חיישן תרמי


36 אינדקס

1 סקירה כללית של ניהול מחשב שולחני

תוכנת HP Client Management Solutions מספקת פתרונות המבוססים על סטנדרטים מקובלים לניהול ולבקרה על מחשבים שולחניים, תחנות עבודה ומחשבים ניידים בסביבת רשת. בשנת 1995 הפכה חברת HP לחלוצה בכל הקשור ליכולת הניהול של מחשב שולחני, הודות להשקעה של ראשוני המחשבים שתמכו ביכולת ניהול מלאה. חברת HP מחזיקה בפטנט על טכנולוגיית יכולת הניהול (Manageability). מאז, הפכה חברת HP לחברה מובילה בתעשייה במאמציה לפתח סטנדרטים ותשתית הדרושים לפריסה, להגדרות תצורה ולניהול של מחשבים שולחניים, תחנות עבודה ומחשבים ניידים. HP מפתחת תוכנת ניהול משלה ופועלת בשיתוף פעולה הדוק עם ספקי פתרונות ניהול כדי להבטיח תאימות בין תוכנת HP Client Management Solutions לבין מוצרים אלה. פתרונות HP Client Management Solutions הנם היבט חשוב של ההתחייבות הנרחבת שלנו לספק פתרונות שיסייעו לך להפחית את העלות הכוללת של בעלות ותחזוקה של מחשבים במהלך מחזור חייהם.

להלן רשימת היכולות והמאפיינים המרכזיים של ניהול מחשב שולחני:

- הגדרת תצורה ראשונית ופריסה
- התקנת מערכת מרחוק
- עדכון וניהול תוכנה
- זיכרון ROM Flash
- תצורה אופציונלית של חומרה
- בקרת נכסים ואבטחה
- הודעות על מקרי כשל והתאוששות

 **הערה:** תמיכה במאפיינים ספציפיים המתוארים במדריך זה עלולה להשתנות לאור השוני בין דגמים וגרסאות תוכנה.

2 הגדרת תצורה ראשונית ופריסה

המחשב מסופק עם תמונת תוכנת מערכת (system software image) מותקנת מראש. לאחר תהליך קצר של "הוצאת התוכנה מהאריזה", יהיה המחשב מוכן לשימוש.

ייתכן שתעדיף להחליף את תמונת התוכנות המותקנות מראש בתוכנות מערכת ויישומים מותאמים אישית. קיימות מספר שיטות לפריסת תמונת תוכנה מותאמת אישית. שיטות אלה כוללות:

- התקנת יישומי תוכנה נוספים לאחר פתיחת תמונת התוכנה המותקנת מראש.
- שימוש בתוכנות פריסה, כגון HP Client Automation Standard Edition, HP Client Automation Enterprise, Edition (מבוסס על טכנולוגיית Radia) או Altiris Deployment Solution, להחלפת התוכנות המותקנות מראש בתצורת תוכנה מותאמת אישית.
- שכפול דיסק קשיח לצורך העתקת התוכן מכונן קשיח אחד למשנהו.

שיטת הפריסה הטובה ביותר תלויה בסביבת טכנולוגית המידע שלך ובתהליכים שבהם אתה משתמש.

מערכת HP Backup and Recovery, ההגדרות מבוססות ה-ROM וחומרת ACPI מספקים סיוע נוסף לשחזור תוכנות מערכת, ניהול תצורה, פתרון בעיות וניהול צריכת חשמל.

הערה: עיין בסעיף [HP Backup and Recovery Manager \(מנהל הגיבוי והשחזור של HP\) בעמוד 11](#) לקבלת מידע אודות יצירת סדרה של תקליטורי שחזור.

HP Software Agent

סוכן הניהול שמשמש את HP Client Automation מהדורות Standard ו-Enterprise טעון מראש במחשב. כאשר תוכנה זו מותקנת, היא מאפשרת תקשורת עם מסוף הניהול של HP.

להתקנת HP Software Agent:

1. לחץ על **Start** (התחל).
2. לחץ על **All Programs** (כל התוכניות).
3. לחץ על **HP Manageability**.
4. לחץ על **Radia Management Agent Readme**.
5. להתקנת HP Software Agent, עיין בהוראות שבקובץ ה-Readme ופעל לפיהן.

HP Software Agent הוא רכיב תשתית מרכזי בהפעלת כל הפתרונות של HP Client Automation. כדי ללמוד אודות רכיבי תשתית אחרים הנחוצים ליישום פתרונות של ניהול תצורה של HP, בקר בכתובת <http://h20229.www2.hp.com/solutions/ascm/index.html>.

Altiris Deployment Solution Agent

תוכנית זו נטענה מראש במחשב. כאשר תוכנה זו מותקנת, היא מאפשרת תקשורת עם מסוף Deployment Solution של מנהל המערכת.

כדי להתקין את Altiris Deployment Solution Agent:

1. לחץ על **Start** (התחל).
2. לחץ על **All Programs** (כל התוכניות).
3. עבור Windows Vista, לחץ על **Install Altiris DAgent** (התקן את Altiris DAgent). עבור Windows XP, לחץ על **Install Altiris AClient** (התקן את Altiris AClient).
4. פעל בהתאם להוראות שעל-גבי המסך כדי להתקין ולהגדיר את התצורה של לקוח Altiris.

סוכן זה הוא רכיב תשתית מרכזי להפעלת Altiris Deployment Solution, המהווה חלק מחבילת Altiris Client Management Suite. כדי ללמוד אודות רכיבי תשתית אחרים הנחוצים ליישום Altiris Client Management Suite, בקר בכתובת <http://www.hp.com/go/easydeploy>.

3 Remote System Installation (התקנת מערכת מרחוק)

Remote System Installation (התקנת מערכת מרחוק) מאפשרת אתחול והגדרה של המערכת באמצעות שימוש בתוכנה ובנתוני הגדרת תצורה הנמצאים בשרת הרשת באמצעות הפעלת סביבת Preboot Execution Environment (PXE). המאפיין Remote System Installation (התקנת מערכת מרחוק) מופעל בדרך כלל ככלי להתקנת והגדרת תצורת המערכת, וניתן להשתמש בו לביצוע המטלות הבאות:

- אתחול כונן קשיח
- פריסת תמונת תוכנה במחשב חדש אחד או יותר
- עדכון מרחוק של BIOS המערכת ב-flash ROM ([זיכרון הבזק Remote ROM Flash בעמוד 15](#))
- קביעת תצורה של הגדרות BIOS המערכת

כדי להפעיל את Remote System Installation (התקנת מערכת מרחוק), הקש **F12** עם הופעת ההודעה **F12 = Network Service Boot** (F12 = אתחול שירות מערכת) בפינה הימנית התחתונה של מסך הסמל של HP בעת אתחול המחשב. פעל על פי ההוראות המוצגות על המסך כדי להמשיך את התהליך. סדר האתחול המשמש כברירת מחדל הוא הגדרת תצורה של ה-BIOS, שניתן לשנותה כך שהמערכת תמיד תנסה לבצע אתחול PXE.

HP מספקת כמה כלים לניהול ועדכון תוכנות במחשבים שולחניים, בתחנות עבודה ובמחשבים ניידים.

- HP Client Management Interface
- HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools Security Manager
- HP Client Automation מהדורות Starter, Standard ו-Enterprise
- HP Client Manager מ-Symantec
- Altiris Client Management Suite
- HP Client Catalog עבור מוצרי Microsoft System Center ו-SMS
- HP Backup and Recovery Manager (מנהל הגיבוי והשחזור של HP)
- מחשבי Intel vPro עם טכנולוגיית Active Management Technology
- Verdiem Surveyor
- HP Proactive Change Notification
- HP Subscriber's Choice

HP Client Management Interface

לא משנה באילו כלי ניהול מערכת משתמשת מחלקת ה-IT שלך, ניהול של נכסי החומרה והתוכנה חשוב לצורך שמירה על עלויות נמוכות ועל עסק יעיל. מנהל ה-IT יכול לגשת ל-HP Client Management Interface על-ידי כתיבה של קובצי script פשוטים ושילוב קובצי script אלה בפתרון הניהול המועדף עליו.

באמצעות ממשק HP Client Management Interface (HP CMI), מחשבים עסקיים חדשים של HP משתלבים ללא תקלות בסביבת ה-IT המנוהלת שלך. HP CMI מספק ממשק שמפשט את ההשתלבות של מחשבים עסקיים של HP עם כלי ניהול מערכת נפוצים בענף (לרבות Microsoft Systems Management Server, IBM Tivoli Software ו-HP Operations) ויישומי ניהול פנים-ארגוניים מותאמים אישית. באמצעות HP CMI, כלי ניהול מערכת ויישומי מערכת יכולים לבקש רשימת מלאי מפורטת של הלקוח, לקבל מידע אודות מצב התקינות ולנהל הגדרות של BIOS המערכת באמצעות קיום תקשורת ישירה עם מחשב הלקוח, ובכך פוחת הצורך בתוכנת סוכן או מחבר לצורך שילוב.

ה-HP CMI מבוסס על הסטנדרטים המקובלים בשוק, לרבות Microsoft Windows Management Interface (MS) (WMI) Web-Based Enterprise Management (WBEM), System Management BIOS (SMBIOS) ו-Advanced Configuration and Power Interface (ACPI). HP CMI הוא טכנולוגיית יסוד המשמשת את ה-HP Client Management Solutions. בעזרת HP CMI, HP מאפשרת לך לבחור באופן גמיש כיצד לנהל את מחשבי הלקוח של HP שברשותך.

כאשר נעשה שימוש ב-HP CMI בשילוב עם תוכנה לניהול מערכת, ה-HP CMI יכול:

- לבקש רשימת מלאי מפורטת של הלקוח – להשיג מידע מפורט אודות המעבדים, הכוננים הקשיחים, הזיכרון, ה-BIOS, מנהלי התקן, לרבות מידע של חיישנים (כגון מהירות המאוורר, מתח וטמפרטורה).
- לקבל מידע אודות מצב התקינות – לבצע רישום למגוון רחב של התראות חומרה ללקוח (כגון התחממות-יתר, מאוורר תקוע ושינויים בתצורת החומרה) שיישלחו למסוף ניהול המערכת, ליישום או למחשב הלקוח המקומי. ההתראות נשלחות בזמן אמת כאשר מתרחשים אירועי חומרה.
- לנהל את הגדרות ה-BIOS של המערכת – לבצע פונקציות F10 מרחוק, לרבות הגדרה ושינוי של סיסמאות ה-BIOS וסדר אתחול המחשב מתוך מסוף הניהול של המערכת או מאחת או כל מערכות הלקוח, ללא צורך לבקר בכל מכונה.

לקבלת מידע נוסף אודות ה-HP Client Management Interface, בקר בכתובת <http://www.hp.com/go/hpcmi>.

HP SoftPaq Download Manager

HP SoftPaq Download Manager הוא ממשק ללא תשלום וקל לשימוש לאיתור ולהורדה של עדכוני תוכנה עבור דגמי מחשב לקוח של HP בסביבתך. ציון הדגמים, מערכת ההפעלה והשפה מאפשר לך לאתר, למיין ולבחור את קובצי ה-softpaq הדרושים במהירות. להורדת HP SoftPaq Download Manager, בקר בכתובת <http://www.hp.com/go/sdm>.

HP System Software Manager

HP System Software Manager (SSM) הוא כלי עזר המסופק ללא תשלום, המאפשר פריסה אוטומטית מרחוק של מנהלי התקן ועדכוני BIOS עבור מחשבים עסקיים של HP הפועלים ברשת. כאשר תוכנית השירות SSM פועלת, היא קובעת בצורה שקטה (ללא התערבות המשתמש) את המהדורות של מנהלי ההתקן וה-BIOS המותקנים בכל מערכת לקוח המחוברת לרשת, ומשווה את רשימת המצאי לערכות SoftPaq של תוכנת המערכת, שנבדקו ואוחסנו במאגר קבצים מרכזי. לאחר מכן, כלי העזר SSM מעדכן באופן אוטומטי ומתאים את מהדורות תוכנות המערכת שמותקנות במחשבים המחוברים לרשת למהדורות הזמינות במאגר הקבצים. מאחר ש-SSM מאפשר הפצה של עדכוני SoftPaq לדגמים הנכונים של מערכות הלקוח בלבד, מנהלי מערכת יכולים להשתמש בצורה בטוחה ויעילה ב-SSM כדי להבטיח שתוכנות המערכת יהיו מעודכנות.

System Software Manager משתלב עם כלי הפצת התוכנות הארגוניים כגון פתרונות של HP Client Automation, HP Client Manager מ-Symantec ו-Microsoft Systems Management Server (SMS). באמצעות SSM, ניתן להפיץ עדכונים שנוצרו על-ידי הלקוח, או התקבלו מספק צד שלישי, ונארוזו בתבנית SSM.

ניתן להוריד את ה-SSM ללא תשלום בכתובת <http://www.hp.com/go/ssm>.

הערה: SSM לא תומך כעת ב-ROM flash מרוחק במערכות שבהן מאופשר Windows Vista BitLocker והמשתמשות במדידות TPM להגנה על מפתחות BitLocker, מאחר ש-flashing של ה-BIOS יבטל את חתימת האמון שאותה יצר BitLocker עבור הפלטפורמה. השבת את BitLocker דרך Group Policy (מדיניות קבוצתית) כדי לבצע flash של ה-BIOS המערכת.

באפשרותך להפעיל תמיכה של BitLocker ללא מדד TPM (תחזוקה פרודוקטיבית כוללת) של ה-BIOS כדי למנוע דחייה של סיסמאות ה-HP. BitLocker ממליצה לשמור גיבוי מאובטח של כתב-האמנה של BitLocker לצורך שחזור במקרה חירום.

HP ProtectTools Security Manager

תוכנת HP ProtectTools Security Manager מספקת מאפייני אבטחה המסייעים בהגנה כנגד גישה לא מורשית למחשב, לרשתות ולנתונים חיוניים. מודולי התוכנה הבאים מספקים פונקציונליות אבטחה משופרת:

- Credential Manager for HP ProtectTools
- Embedded Security for HP ProtectTools
- Java Card Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Device Access Manager for HP ProtectTools
- HP ProtectTools עבור File Sanitizer
- HP ProtectTools עבור Privacy Manager

מודולי התוכנה הזמינים עבור המחשב שברשותך עשויים להשתנות בהתאם לדגם. לדוגמה, מודול התוכנה Embedded Security for HP ProtectTools זמין רק עבור מחשבים שבהם מותקן שבב האבטחה המשובצת מסוג Trusted Platform Module (TPM).

מודולי התוכנה של HP ProtectTools עשויים להיות מותקנים מראש, טעונים מראש או זמינים להורדה מהאתר של HP. עבור מחשבים שולחניים נבחרים של HP Compaq, HP ProtectTools זמין כאפשרות לשיווק נלווה. לקבלת מידע נוסף, בקר בכתובת <http://www.hp.com/products/security>.

Standard-ו Starter מהדורות HP Client Automation

HP Client Automation הוא פתרון חומרה ותוכנה קל לשימוש ומהיר לפריסה עבור סביבות Windows, Windows Vista, HP Thin Client-ו XP, המספק בסיס איתן לדרישות עתידיות. הוא מסופק בשתי מהדורות:

- מהדורת Starter Edition היא מוצר המופץ בחינם, לניהול מחשבים שולחניים, מחשבים ניידים ותחנות עבודה של HP, והמספק מלאי של חומרה ותוכנה, שלט-רחוק, ניטור התראות של HP, עדכונים ל-HP BIOS ולמנהלי התקן, אינטגרציה עם כלי HP Protect Tools ותמיכה מורחבת עבור Intel AMT. מהדורת Starter Edition גם תומכת בפריסה וניהול של HP Thin Clients.

- מהדורת Standard Edition, הזמינה לרכישה, כוללת את כל התפקודיות המסופקת במהדורה הבסיסית ומוסיפה פריסה והעברה של Windows, יכולות ניהול תיקונים, הפצת תוכנות ומדידת שימוש בתוכנה.

HP Client Automation מהדורות Starter-ו Standard מספק נתיב העברה ל-HP Client Automation Enterprise Edition (מבוסס על טכנולוגיית Radia) עבור ניהול אוטומטי של סביבות IT גדולות, הטרוגניות ומשתנות.

לקבלת מידע נוסף אודות הפתרונות של HP Client Automation, בקר בכתובת <http://www.hp.com/go/client>.

HP Client Automation Enterprise Edition

HP Client Automation Enterprise Edition הוא פתרון מבוסס מדיניות, המאפשר למנהלים לנהל מלאי, לפרוס, לתקן ולנהל באופן שוטף תוכנות ותוכן בפלטפורמות לקוח הטרוגניות. באמצעות HP Client Automation Enterprise Edition, מומחה ה-IT יכול:

- למכן את תהליך ניהול מחזור החיים כולו, מהגילוי, הפריסה והניהול השוטף עד להעברה וסילוק

- לפרוס באופן אוטומטי ולנהל באופן שוטף את כלל התוכנות (מערכות ההפעלה, היישומים, התיקונים, ההגדרות והתוכן) במצב הרצוי

- לנהל תוכנות בכל התקן כמעט, לרבות מחשבים שולחניים, תחנות עבודה ומחשבים ניידים, בתשתית הטרוגנית או עצמאית

- לנהל תוכנות ברוב מערכות ההפעלה

הודות לניהול תצורה שוטף, לקוחות HP מדווחים על חיסכון משמעותי בעלויות IT, על קיצור התהליך של הוצאת תוכנות ותכנים לשוק ועל הגברת פרודוקטיביות המשתמשים ושביעות רצונם.

לקבלת מידע נוסף אודות הפתרונות של HP Client Automation, בקר בכתובת <http://www.hp.com/go/client>.

Symantec-מ HP Client Manager

תוכנת Symantec-מ HP Client Manager, שפותחה בשיתוף עם Altiris, זמינה ללא תשלום עבור כל דגמי המחשבים השולחניים העסקיים, תחנות העבודה ומחשבי המחברת הנתמכים של SSM. HP משולב בתוך HP Client Manager, ומאפשר לבצע מעקב, ניטור וניהול ריכוזיים של כל רכיבי החומרה של מחשבי לקוח של HP.

השתמש ב-Symantec-מ HP Client Manager לביצוע הפעולות הבאות:

- קבלת מידע חשוב על רכיבי חומרה, כגון CPU, זיכרון, וידאו והגדרות אבטחה
 - ניטור תקינות המערכת לפתרון בעיות לפני התרחשותן
 - רכישה והתקנה של עדכונים למנהלי התקן ול-BIOS באופן אוטומטי, מבלי לבקר בכל מחשב
 - קביעת תצורה מרחוק של הגדרות ה-BIOS והגדרות אבטחה
 - הפיכת תהליכים לאוטומטיים, כדי לפתור בעיות חומרה במהירות
- שילוב הדוק עם הכלים של HP Instant Support מפחית את הזמן הנדרש לפתרון בעיות חומרה.
- Diagnostics (אבחון) – הפעל והצג מרחוק דוחות במחשבים שולחניים, מחשבים ניידים ותחנות עבודה של HP
 - System Health Scan (סריקת תקינות המערכת) – בדוק אם קיימות בעיות חומרה נפוצות בבסיס המותקן של מערכות הלקוח של HP
 - Active Chat (צ'אט פעיל) – התחבר לתמיכה ללקוחות של HP כדי לפתור בעיות
 - HP Knowledgebase – קישור למידע ממומחים
 - תהליך איסוף ושליחה אוטומטי של SoftPaq לפתרון מהיר של בעיות חומרה
 - זיהוי, ספירת מלאי ואתחול של מערכות באמצעות שבב האבטחה המשובץ של HP ProtectTools
 - אפשרות להציג באופן מקומי התראות בנוגע לתקינות במערכת הלקוח
 - דיווח של מידע בסיסי אודות ספירת מלאי עבור מחשבי לקוח שאינם של HP
 - התקנה והגדרת התצורה של שבב האבטחה TPM
 - תזמון של גיבוי ושחזור לקוח באופן ממורכז
 - תמיכה בתוספות לניהול Intel AMT

לקבלת מידע נוסף אודות Symantec-מ HP Client Manager, בקר בכתובת <http://www.hp.com/go/clientmanager>.

ערכת Altiris Client Management Suite

ערכת Altiris Client Management Suite היא פתרון קל לשימוש לניהול מחזור חיים מלא של תוכנות במחשבים שולחניים, מחשבים ניידים ותחנות עבודה. Altiris Client Management Suite Level 1 כוללת את מוצרי Altiris הבאים:

- Inventory Solution
- Deployment Solution
- Software Delivery Solution
- Patch Management Solution
- Application Metering Solution
- Application Management Solution
- Carbon Copy Solution

לקבלת מידע נוסף אודות ערכת Altiris Client Management Suite, בקר בכתובת <http://www.altiris.com/Products/ClientManagementSuite.aspx>.

HP Client Catalog SMS עבור מוצרי Microsoft System Center ו-

HP Client Catalog מאפשר למומחי IT המשתמשים במוצרי Microsoft למכנ את הפריסה של עדכוני תוכנה של HP (Softpaqs) במחשבים עסקיים של HP. קובץ הקטלוג מכיל מידע פלטפורמה מפורט אודות מחשבים שולחניים, מחשבים ניידים ותחנות עבודה של HP. ניתן להשתמש בקובץ יחד עם מאפייני המצאי והעדכון המותאמים אישית של מוצרי Microsoft, כדי לספק מנהל התקן ועדכוני תיקונים אוטומטיים לניהול מחשבי לקוח של HP.

מוצרי Microsoft בהם תומך HP Client Catalog כוללים:

- System Center Configuration Manager 2007
- System Center Essentials 2007
- Systems Management Server (SMS) 2003 R2

לקבלת מידע נוסף אודות HP Client Catalog for SMS, בקר בכתובת <http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html>.

HP Backup and Recovery Manager (מנהל הגיבוי והשחזור של HP)

ה-HP Backup and Recovery Manager (מנהל הגיבוי והשחזור של HP) הינו יישום רב-תכליתי וקל לשימוש, המאפשר לך לגבות ולשחזר את הכונן הקשיח הראשי במחשב. יישום זה פועל בתוך Windows ויוצר גיבויים של Windows, כל היישומים וכל קובצי הנתונים. ניתן לתכנן גיבויים כך שיופיעו באופן אוטומטי במרווחים מוגדרים, או שיופעלו באופן ידני. ניתן לשמור בארכיון קבצים חשובים בנפרד מגיבויים רגילים.

HP Backup and Recovery Manager (מנהל הגיבוי והשחזור של HP) מותקן מראש על כונן C: ויוצר Recovery Partition (מחיצת שחזור).

ניתן להעתיק Recovery Points (נקודות שחזור) וגיבויי קבצים לתקליטורים או לתקליטורי DVD, ואת כל הגיבויים ניתן להעתיק לרשת או לכוננים קשיחים משניים.

HP ממליצה על יצירת Recovery Disc Set (ערכת תקליטורי שחזור) מיד לפני השימוש במחשב ועל קביעת גיבויי Recovery Point (נקודת שחזור) באופן אוטומטי וקבוע.

ליצירת ה-Recovery Disc Set (ערכת תקליטורי שחזור):

1. לחץ על **Start** (התחל) < **HP Backup and Recovery** (גיבוי ושחזור של HP) < **HP Backup and Recovery Manager** (מנהל הגיבוי והשחזור של HP) כדי לפתוח את Backup and Recovery Wizard (אשף הגיבוי והשחזור) ולאחר מכן לחץ על **Next** (הבא).

2. לחץ על **Create a set of recovery discs (Recommended)** (צור סדרה של תקליטורי שחזור (מומלץ)) ולאחר מכן לחץ על **Next** (הבא).

3. פעל בהתאם להוראות המופיעות באשף.

לקבלת מידע נוסף אודות השימוש ב-HP Backup and Recovery Manager (מנהל הגיבוי והשחזור של HP), עיין ב-*HP Backup and Recovery Manager User Guide* (מדריך למשתמש של מנהל הגיבוי והשחזור של HP) באמצעות בחירה ב-**Start** (התחל) < **HP Backup and Recovery** (גיבוי ושחזור של HP) < **HP Backup and Recovery Manager Manual** (מדריך למנהל הגיבוי והשחזור של HP).

הערה: באפשרותך להזמין ערכת תקליטורי שחזור מ-HP על-ידי פנייה אל מרכז התמיכה של HP. בקר באתר האינטרנט שלהלן, בחר את האזור שלך ולחץ על הקישור **Technical support after you buy** (תמיכה טכנית לאחר הקנייה) תחת הכותרת **Call HP** (יצירת קשר עם HP), כדי להשיג את מספר הטלפון של מרכז התמיכה במדינה/אזור שלך.

http://welcome.hp.com/country/us/en/wwcontact_us.html

טכנולוגיית ניהול

הדגמים כוללים את טכנולוגיית vPro או טכנולוגיה סטנדרטית. שתיהן מאפשרות גילוי, תיקון והגנה טובים יותר של נכסי מחשב ברשת. שתי הטכנולוגיות מאפשרות לנהל מחשבים בין אם המערכת מופעלת, כבויה או שמערכת ההפעלה מנותקת.

מאפייני טכנולוגיות הניהול כוללים:

- מידע אודות מלאי החומרה
- התראה
- ניהול צריכת חשמל – הפעלה/כיבוי, חשמל של מעגל
- אבחון ותיקון מרחוק
 - Serial-over-LAN – מאפשר שליטה ממסוף במחשב מרוחק במהלך שלב האתחול שלו
 - IDE-Redirect – מאפשר אתחול של המערכת מכונן אתחול, דיסק או תמונת ISO מרוחקים
- בידוד ושחזור מבוססי-חומרה – הגבלה או ניתוק גישה לרשת של מחשבים, אם מזוהה פעילות דמויית-וירוס

הערה: לסקירה כללית של טכנולוגיית Intel vPro, בקר בכתובת <http://www.intel.com/vpro>.

למידע ספציפי ל-HP אודות טכנולוגיית Intel vPro, עיין ב-White papers (סקירה טכנית) בכתובת <http://www.hp.com/support>. בחר את המדינה/אזור והשפה הרצויים, בחר **See support and troubleshooting information** (ראה מידע אודות תמיכה ופתרון בעיות), הזן את מספר הדגם של המחשב והקש **Enter**. בקטגוריה **Resources** (משאבים) לחץ על **Manuals (guides, supplements, addendums, etc.)** (מדריכים למשתמש (מדריכים, חומר משלים, נספחים וכו')). תחת **Quick jump to manuals by category** (מעבר מהיר למדריכים למשתמש לפי קטגוריה), לחץ על **White papers** (סקירה טכנית).

טכנולוגיות ניהול זמינות כוללות:

- AMT (לרבות DASH 1.0)
- ASF

ייתכן שלא ניתן יהיה להגדיר את טכנולוגיות ASF ו-AMT בו-זמנית, אך שתיהן נתמכות.

להגדרת מערכות Intel vPro עבור AMT או ASF:

1. הפעל או הפעל מחדש את המחשב. במערכת ההפעלה Windows של Microsoft, לחץ על **Start** (התחל) < **Shut Down** (כיבוי) < **Restart** (הפעלה מחדש).
2. מיד עם הפעלת המחשב, הקש על המקש החם **Ctrl+P**, לפני שהמחשב מאתחל למערכת ההפעלה.

הערה: אם לא הקשת **Ctrl+P** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב ולהקיש שוב על **Ctrl+P** לפני שהמחשב מאתחל למערכת ההפעלה כדי לגשת לתוכנית השירות.

מקש חם זה מפעיל את כלי העזר Intel Management Engine BIOS Execution (MEBx). כלי עזר זה מאפשר למשתמש להגדיר היבטים שונים של טכנולוגיית הניהול. חלק מאפשרויות התצורה מפורטות להלן:

- תפריט Main (ראשי)
 - Intel ® ME Configuration (תצורת Intel ® ME)
 - Intel ® AMT Configuration (תצורת Intel ® AMT)
 - Change Intel ® ME Password (שינוי סיסמה של Intel ® ME)
 - Exit (יציאה)
- Intel ® ME Platform Configuration (תצורה של Intel ® ME Platform)
 - Intel ® ME State Control (בקרת מצב של Intel ® ME) (הפעלה/השבתה)
 - Intel ® ME Firmware Local Update (עדכון מקומי של קושחת Intel ® ME) (הפעלה/השבתה)
 - Intel ® ME Features Control (בקרת מאפיינים של Intel ® ME)
 - Intel ® ME Power Control (בקרת צריכת חשמל של Intel ® ME)
- Intel ® AMT Configuration (תצורת Intel ® AMT)
 - Host Name (שם מארח)
 - TCP/IP
 - Provision Model (Enterprise, SMB) (מודל אספקה (ארגונים, עסקים קטנים ובינוניים))
 - Setup and Configuration (התקנה ותצורה)
 - Un-Provision (ביטול אספקה)
 - SOL/IDE-R (הפעלה/השבתה)
 - Password Policy (מדיניות סיסמאות)
 - Secure Firmware Update (עדכון קושחה מאובטחת) (הפעלה/השבתה)
 - Set PRTC (הגדרת PRTC)
 - Idle Timeout (פסק זמן לאחר חוסר פעילות)
- Change Intel ® ME Password (שינוי סיסמת Intel ® ME) (HP ממליצה לשנות סיסמה זו. הסיסמה המוגדרת כברירת המחדל היא **admin**.)

כדי לנהל מרחוק מערכות AMT, על המנהל להשתמש במסוף מרוחק שתומך ב-AMT. מסופי ניהול לארגונים זמינים מספקים כגון HP, Altiris ו-Microsoft SMS. במצב SMB (עסק קטן/בינוני), מחשב הלקוח מספק ממשק של דפדפן אינטרנט. כדי לגשת למאפיין זה, פתח דפדפן מכל מערכת אחרת ברשת והזן `http://host_name:16992` כאשר `host_name` הוא השם המוקצה למערכת. לחלופין, ניתן להשתמש בכתובת ה-IP במקום בשם המחשב המארח.

Verdiem Surveyor

Verdiem Surveyor הוא פתרון תוכנה המסייע בניהול עלויות צריכת חשמל של מחשבים. ה-Surveyor מודד ומדווח כמה חשמל צורך כל מחשב. בנוסף הוא מספק בקרה על הגדרות החשמל של המחשב וכך מאפשר למנהלי מערכות ליישם בקלות אסטרטגיות לחיסכון בחשמל ברשתות שתחת ניהולם. ניתן להוריד מאתר התמיכה של HP את חבילת HP SoftPaq הכוללת את סוכן ה-Surveyor ולהתקינה על דגמים של מחשבים שולחניים מסחריים נתמכים. ניתן לרכוש רישיונות Surveyor לניהול מחשבים באמצעות נציג HP במדינה/אזור שלך.

HP Proactive Change Notification

התוכנית Proactive Change Notification משתמשת באתר האינטרנט Subscriber's Choice כדי לבצע מראש ובאופן אוטומטי את הפעולות הבאות:

- שליחת הודעות דואר אלקטרוני של Proactive Change Notification (PCN) המדווחות על שינויים ברכיבי חומרה ותוכנה ברוב המחשבים והשרתים המסחריים, עד 60 יום מראש
 - שליחת הודעות דואר אלקטרוני הכוללות עלונים ללקוח, דפי עזר, הערות ללקוח, עלוני אבטחה והתראות על מנהלי התקן עבור רוב המחשבים והשרתים המסחריים
- יצירת פרופיל אישי כדי להבטיח שרק אתה אישית תקבל את המידע הדרוש לסביבת טכנולוגיית מידע ספציפית. לקבלת מידע נוסף אודות תוכנית Proactive Change Notification וליצירת פרופיל מותאם אישית, בקר בכתובת <http://h30046.www3.hp.com/subhub.php>

Subscriber's Choice

Subscriber's Choice הוא שירות מבוסס לקוח של HP.

בהתאם לפרופיל שלך, HP תספק לך עצות אישיות לגבי מוצרים, מאמרים ו/או מנהלי התקן והתראות/הודעות בנושא תמיכה.

שירות מנהלי ההתקן וההתראות/הודעות בנושאי תמיכה ישלח לך הודעות דואר אלקטרוני, שידווחו לך כאשר המידע שאליו נרשמת כמנוי בפרופיל שלך יהיה זמין לעיון ואחזור. לקבלת מידע נוסף אודות תוכנית Subscriber's Choice וליצירת פרופיל מותאם אישית, בקר בכתובת <http://h30046.www3.hp.com/subhub.php>.

פתרונות שאינם בשימוש

שתי חבילות תוכנה, Altiris Local Recovery ו-Dantz Retrospect, לא יסופקו יותר עם המחשבים השולחניים, המחשבים הניידים או תחנות העבודה של HP. מחשבים שולחניים עסקיים, מחשבים ניידים ותחנות עבודה המשווקים משנת 2006 יסופקו עם HP Backup and Recovery Manager (מנהל הגיבוי והשחזור של HP).

ה-BIOS של המחשב מאוחסן בזיכרון Flash ROM (זיכרון לקריאה בלבד) הניתן לתיכנות. על-ידי הגדרת סיסמת הגדרות בתוכנית השירות Computer Setup (הגדרות המחשב) (F10), תוכל להגן על זיכרון ה-ROM מפני עדכון או מפני דריסה בלתי מכוונת. הדבר חשוב כדי להבטיח את שלמות פעולתו של המחשב. אם תרצה או תידרש לבצע שדרוג של ה-BIOS, תוכל להוריד את תמונות ה-BIOS העדכניות ביותר מדף מנהלי ההתקן והתמיכה של HP, בכתובת <http://www.hp.com/support/files>.

△ **זהירות:** להגנה מרבית על ה-ROM, הקפד ליצור סיסמת הגדרות. סיסמת ההגדרות מונעת שדרוגים לא מורשים של זיכרון System Software Manager. ROM מאפשר למנהל המערכת להגדיר סיסמת הגדרות במחשב אחד או במספר מחשבים בו-זמנית. לקבלת מידע נוסף, בקר בכתובת <http://www.hp.com/go/ssm>.

זיכרון הבזק Remote ROM Flash

Remote ROM Flash מאפשר למנהל המערכת לשדרג בצורה בטוחה את ה-BIOS במחשבי HP מרוחקים, ישירות מתוך עמדת ניהול רשת מרכזית. יכולתו של מנהל המערכת לבצע משימה זו מרוחק במספר מחשבים, מאפשרת פריסה עקבית ושליטה טובה יותר בתמונות ה-BIOS במחשבי HP דרך הרשת. כמו כן, היא מאפשרת להגביר את התפוקה ולצמצם בעלויות הבעלות.

📖 **הערה:** SSM לא תומך כעת ב-ROM flash מרוחק במערכות שבהן מאופשר Windows Vista BitLocker והמשתמשות במדידות TPM להגנה על מפתחות BitLocker, מאחר ש-flashing של ה-BIOS יבטל את חתימת האמון שאותה יצר BitLocker עבור הפלטפורמה. השבת את BitLocker דרך Group Policy (מדיניות קבוצתית) כדי לבצע flash של BIOS המערכת.

כדי לנצל את יתרונות Remote ROM Flash, על המחשב להיות מופעל, או שיש להפעילו באמצעות יקיצה מרוחק (Remote Wakeup).

לקבלת מידע נוסף אודות Remote ROM Flash, היעזר בתוכנה HP Client Manager Software או ב-System Software Manager בכתובת <http://www.hp.com/go/ssm>.

HPQFlash

תוכנית השירות HPQFlash משמשת לעדכון מקומי או לשחזור BIOS המערכת במחשבים יחידים, באמצעות מערכת ההפעלה Windows.

לקבלת מידע נוסף אודות HPQFlash, בקר בכתובת <http://www.hp.com/support/files> והזן את מספר הדגם של המחשב כשתופיע הנחיה לכך.

Boot Block Emergency Recovery Mode

(מצב שחזור חירום של בלוק אתחול)

Boot Block Emergency Recovery Mode (מצב שחזור חירום של בלוק אתחול) מאפשר שחזור של המערכת במקרה לא סביר של כשל בזיכרון ROM Flash. לדוגמה, אם התרחשה הפסקת חשמל במהלך שדרוג ה-ROM BIOS, Flash לא יהיה שלם. פעולה זו תוציא את BIOS המערכת מכלל שימוש. Boot Block (בלוק האתחול) הוא אזור מוגן-Flash של זיכרון ה-ROM, שמכיל קוד המשמש לבדיקת תקפות תמונת ה-BIOS של המערכת כאשר המערכת מופעלת.

- אם תמונת ה-BIOS תקפה, המערכת מתחילה לפעול כרגיל.
- אם תמונת ה-BIOS אינה תקפה, מצב Failsafe Boot Block BIOS (אל-כשל של בלוק האתחול) מספק תמיכה מספקת כדי לחפש קובצי תמונת BIOS באמצעי אחסון נשלפים. אם נמצא קובץ תמונת BIOS מתאים, הוא מבצע Flash אוטומטי לתוך ה-ROM.

כאשר מ זוהה תמונת BIOS לא תקפה של המערכת, נורית ההפעלה של המערכת תהבהב באדום 8 פעמים, הבהוב אחד בכל שנייה. במקביל, הרמקול ישמיע 8 צפצופים. אם החלק של ROM המערכת שמכיל את תמונת ה-ROM של אפשרות הווידאו אינו פגום, **Boot Block Emergency Recovery Mode** (מצב שחזור חירום של בלוק האתחול) יוצג על-גבי המסך.

כדי לאפשר למערכת להתאושש לאחר כניסה ל-Boot Block Emergency Recovery Mode (מצב שחזור חירום של בלוק האתחול), פעל בהתאם לשלבים הבאים:

1. כבה את אספקת החשמל.
2. הכנס תקליטור או התקן Flash של USB, שמכילים את קובץ תמונת ה-BIOS הרצויה בספריית הבסיס.

הערה: המדיה צריכה להיות מאותחלת באמצעות מערכת הקבצים FAT12, FAT16 או FAT32.

3. הפעל את המחשב.
 - אם לא נמצאה תמונת BIOS מתאימה, תתבקש להכניס אמצעי אחסון שמכיל קובץ תמונת BIOS.
 - אם המערכת מתכנתת שוב בהצלחה את ה-ROM, היא תכבה באופן אוטומטי.
4. הוצא את המדיה הנשלפת ששימשה לשדרוג ה-BIOS.
5. חדש את אספקת החשמל כדי להפעיל מחדש את המחשב.

הערה: BitLocker מונע מ-Windows Vista לבצע אתחול כאשר בכונן אופטי נמצא תקליטור המכיל את קובץ תמונת ה-BIOS. אם BitLocker מאופשר, הוצא תקליטור זה לפני שתנסה לבצע אתחול ל-Windows Vista.

ההליכים הבאים מאפשרים למנהל המערכת יכולת להעתיק בקלות רבה תצורת הגדרות מערכת אחת למחשבים אחרים מאותו דגם. הדבר מאפשר לבצע הגדרת תצורה מהירה ועקבית של מספר מחשבים.

הערה: שני ההליכים דורשים כונן תקליטונים או כונן USB flash נתמך.

העתקה למחשב אחד

זהירות: תצורת ההגדרות ספציפית לכל דגם. מערכת הקבצים עשויה להיפגם אם מחשב המקור ומחשב היעד אינם מאותו דגם. לדוגמה, אין להעתיק את תצורת ההתקנה ממחשב מדגם dc7xxx למחשב מדגם dx7xxx.

1. בחר תצורת הגדרות להעתקה. כבה את המחשב. במערכת ההפעלה Windows, לחץ על **Start** (התחל) < **Shut Down** (כיבוי) < **Shut Down** (כיבוי).
 2. אם אתה משתמש בהתקן USB flash media, הכנס אותו כעת.
 3. הפעל את המחשב.
 4. עם הפעלת המחשב, הקש **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי להיכנס לתוכנית השירות Computer Setup. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.
- הערה:** אם לא הקשת **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב ולהקיש שוב על **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי לגשת לתוכנית השירות.
5. אם אתה משתמש בתקליטון, הכנס אותו כעת.
 6. לחץ על **File** (קובץ) < **Replicated Setup** (הגדרות משוכפלות) < **Save to Removable Media** (שמור במדיה נשלפת). פעל בהתאם להוראות שעל-גבי המסך כדי ליצור את תקליטון התצורה או את התקן USB Flash Media.
 7. כבה את המחשב שיש להגדיר, והכנס את תקליטון התצורה או את התקן USB flash media.
 8. הפעל את המחשב שיש להגדיר.
 9. עם הפעלת המחשב, הקש **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי להיכנס לתוכנית השירות Computer Setup. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.
 10. לחץ על **File** (קובץ) < **Replicated Setup** (הגדרות משוכפלות) < **Restore from Removable Media** (שחזר ממדיה נשלפת), ולאחר מכן פעל בהתאם להוראות שעל-גבי המסך.
 11. הפעל מחדש את המחשב לאחר השלמת קביעת התצורה.

העתקה למספר מחשבים

זהירות: תצורת ההגדרות ספציפית לכל דגם. מערכת הקבצים עשויה להיפגם אם מחשב המקור ומחשב היעד אינם מאותו דגם. לדוגמה, אין להעתיק את תצורת ההתקנה ממחשב מדגם dc7xxx למחשב מדגם dx7xxx.

בשיטה זו דרוש מעט יותר זמן להכנת תקליטון התצורה או התקן USB flash media, אך העתקת התצורה למחשבי היעד מהירה יותר באופן משמעותי.

הערה: להליך זה או ליצירת התקן USB flash media שניתן לאתחול דרוש תקליטון שניתן לאתחול. אם לא ניתן להשתמש ב-Windows XP ליצירת תקליטון שניתן לאתחול, השתמש בשיטה להעתקה למחשב יחיד (עיין בסעיף [העתקה למחשב אחד בעמוד 17](#)).

1. צור תקליטון או התקן USB flash media שניתנים לאתחול. עיין בסעיף [התקני USB flash media נתמכים בעמוד 18](#) או בסעיף [התקן USB flash media שאינו נתמך בעמוד 20](#).

זהירות: לא כל המחשבים ניתנים לאתחול מהתקן USB flash media. אם סדר האתחול בתוכנית השירות Computer Setup (F10) (הגדרות המחשב) מציין את התקן ה-USB לפני הכונן הקשיח, ניתן לאתחול את המחשב מהתקן USB Flash Media. אחרת, יש להשתמש בתקליטון שניתן לאתחול.

2. בחר תצורת הגדרות להעתקה. כבה את המחשב. במערכת ההפעלה Windows, לחץ על **Start** (התחל) < **Shut Down** (כיבוי) < **Shut Down** (כיבוי).

3. אם אתה משתמש בהתקן USB flash media, הכנס אותו כעת.

4. הפעל את המחשב.

5. עם הפעלת המחשב, הקש **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי להיכנס לתוכנית השירות Computer Setup. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.

הערה: אם לא הקשת **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב ולהקיש שוב על **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי לגשת לתוכנית השירות.

6. אם אתה משתמש בתקליטון, הכנס אותו כעת.

7. לחץ על **File** (קובץ) < **Replicated Setup** (הגדרות משוכפלות) < **Save to Removable Media** (שמור במדיה נשלפת). פעל בהתאם להוראות שעל-גבי המסך כדי ליצור את תקליטון התצורה או את התקן USB Flash Media.

8. הורד כלי עזר של BIOS לשכפול ההגדרות (repset.exe) והעתק אותו לתקליטון התצורה או להתקן USB flash media. להשגת כלי עזר זה, בקר בכתובת <http://welcome.hp.com/country/us/en/support.html> והזן את מספר הדגם של המחשב.

9. בתקליטון התצורה או בהתקן USB flash media, צור קובץ bat.autoexec שמכיל את הפקודה הבאה:

```
repset.exe
```

10. כבה את המחשב שיש להגדיר. הכנס את תקליטון התצורה, או את התקן USB flash media, והפעל את המחשב. תוכנית השירות של התצורה תופעל באופן אוטומטי.

11. הפעל מחדש את המחשב לאחר השלמת קביעת התצורה.

יצירת התקן שניתן לאתחול

התקני USB flash media נתמכים

התקנים נתמכים כוללים תמונה מותקנת מראש כדי לפשט את תהליך הפיכתם להתקנים שניתנים לאתחול. כל התקני USB flash media של HP או של Compaq, רוב ההתקנים האחרים כוללים תמונה מותקנת מראש זו. אם בהתקן ה-

USB flash media שבשימוש לא קיימת תמונה זו, השתמש בהליך המפורט בהמשך סעיף זה (עיין בסעיף [התקן USB flash media שאינו נתמך בעמוד 20](#)).

כדי ליצור התקן USB flash media שניתן לאתחול, דרושים לך:

- התקן USB flash media נתמך
- תקליטון DOS שניתן לאתחול עם התוכניות FDISK ו-SYS (אם התוכנית SYS אינה זמינה, ניתן להשתמש בתוכנית FORMAT, אך כל הקבצים הקיימים בהתקן USB flash media יאבדו).
- מחשב הניתן לאתחול מהתקן USB flash media

זהירות: ייתכן שחלק מהמחשבים הישנים יותר אינם ניתנים לאתחול מהתקן USB flash media. אם סדר האתחול בתוכנית השירות Computer Setup (F10) (הגדרות המחשב) מצוין את התקן ה-USB לפני הכונן הקשיח, ניתן לאתחל את המחשב מהתקן USB Flash Media. אחרת, יש להשתמש בתקליטון שניתן לאתחול.

1. כבה את המחשב.
2. הכנס את התקן USB flash media לאחת מיציאות ה-USB של המחשב, והסר את כל התקני אחסון ה-USB האחרים, פרט לכונני תקליטונים של USB.
3. הכנס תקליטון שניתן לאתחול עם FDISK.COM ו-SYS.COM או FORMAT.COM לכונן תקליטונים והפעל את המחשב כדי לבצע אתחול מתקליטון ה-DOS.
4. הפעל את FDISK מתוך שורת הפקודה **A:** על-ידי הקלדת **FDISK** והקשה על **Enter**. אם תתבקש, לחץ על **Yes** (כן) (**Y**) כדי להפעיל תמיכה בדיסקים גדולים.
5. בחר באפשרות [5] כדי להציג את הכוננים במערכת. התקן USB flash media יהיה הכונן שגודלו קרוב ביותר לגודל של אחד הכוננים המוצגים. בדרך כלל יהיה זה הכונן האחרון ברשימה. שים לב לאות הכונן.
כונן התקן USB flash media: _____

זהירות: אם הכונן אינו תואם להתקן ה-USB flash media, אל תמשיך. במקרה כזה אתה עלול לאבד נתונים. חפש התקני אחסון נוספים בכל יציאות ה-USB. אם תאתר התקנים כאלה, הפעל את המחשב מחדש והמשך משלב 4. אם לא תמצא אף התקן, ייתכן שהמערכת אינה תומכת בהתקן USB flash media, או שהתקן USB flash media פגום. אין להמשיך ולנסות להפוך את התקן USB flash media להתקן שניתן לאתחול.

6. צא מ-FDISK על-ידי הקשה על מקש **Esc** כדי לחזור לשורת הפקודה **A:**.
7. אם תקליטון DOS שניתן לאתחול מכיל את COM.SYS, עבור לשלב 8. אחרת, עבור לשלב 9.
8. בשורת הפקודה **A:** הזן **×** SYS כאשר **x** מייצג את הכונן שצוינה לעיל.

זהירות: ודא שהזנת את אות הכונן הנכונה עבור התקן USB flash media.

9. לאחר העברת קובצי המערכת, התוכנית SYS תחזור לשורת הפקודה **A:**. עבור לשלב 13.
9. העתק קבצים שברצונך לשמור מהתקן USB flash media לספרייה זמנית בכונן אחר (לדוגמה, הכונן הקשיח הפנימי של המערכת).
10. בשורת הפקודה **A:** הזן **×** /S FORMAT כאשר **x** מייצג את הכונן שצוינה לפני כן.

זהירות: ודא שהזנת את אות הכונן הנכונה עבור התקן USB flash media.

התוכנית FORMAT תציג הודעה אחת או יותר, ותשאל אותך בכל פעם אם ברצונך להמשיך. הקש **Y** בכל פעם. התוכנית FORMAT תפרמט את התקן USB flash media, תוסיף את קובצי המערכת ותבקש תווית לאמצעי האחסון.

11. הקש **Enter** אם אינך מעוניין בתווית, או הזן תווית אם רצונך בכך.

12. העתק קבצים ששמרת בשלב 9 בחזרה להתקן USB flash media .

13. הוצא את התקליטון והפעל את המחשב מחדש. המחשב יבצע אתחול מהתקן USB flash media ככונן C.

הערה: סדר האתחול המוגדר כברירת מחדל משתנה ממחשב למחשב, וניתן לשנותו בתוכנית השירות Computer Setup (F10) (הגדרות המחשב).

אם השתמשת בגרסת DOS מתוך Windows 9, ייתן שתראה את מסך הסמל של Windows למשך זמן קצר. אם אינך רואה מסך זה, הוסף קובץ באורך אפס בשם LOGO.SYS לספריית השורש של התקן USB flash media.

חזור לסעיף [העתקה למספר מחשבים בעמוד 18](#).

התקן USB flash media שאינו נתמך

כדי ליצור התקן USB flash media שניתן לאתחול, דרושים לך:

- התקן USB flash media
- תקליטון DOS שניתן לאתחול עם התוכניות FDISK ו-SYS (אם התוכנית SYS אינה זמינה, ניתן להשתמש בתוכנית FORMAT, אך כל הקבצים הקיימים בהתקן USB flash media יאבדו).
- מחשב הניתן לאתחול מהתקן USB flash media

זהירות: ייתכן שחלק מהמחשבים הישנים יותר אינם ניתנים לאתחול מהתקן USB flash media. אם סדר האתחול בתוכנית השירות Computer Setup (F10) (הגדרות המחשב) מציין את התקן ה-USB לפני הכונן הקשיח, ניתן לאתחל את המחשב מהתקן USB Flash Media. אחרת, יש להשתמש בתקליטון שניתן לאתחול.

1. אם קיימים כרטיסי PCI במערכת, שמחברים אליהם כונני SCSI, SATA RAID או SATA, כבה את המחשב ונתק את כבל המתח.

זהירות: על כבל המתח להיות מנותק.

2. פתח את המחשב והוצא את כרטיסי ה-PCI.

3. הכנס את התקן USB flash media לאחת מיציאות ה-USB של המחשב, והסר את כל התקני אחסון ה-USB האחרים, פרט לכונני תקליטונים של USB. סגור את כיסוי המחשב.

4. חבר את כבל המתח והפעל את המחשב.

5. עם הפעלת המחשב, הקש **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי להיכנס לתוכנית השירות Computer Setup. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.


הערה: אם לא הקשת **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב ולהקיש שוב על **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי לגשת לתוכנית השירות.

6. עבור אל **Advanced** (מתקדם) < **PCI Devices** (התקני PCI) כדי להשבית את בקרי PATA ו-SATA. בעת השבתת בקר SATA, שים לב ל-IRQ שאליו מוקצה הבקר. יהיה עליך להקצות מחדש את ה-IRQ בשלב מאוחר יותר. יציאה מתוכנית ההגדרות מאשרת את השינויים.

SATA IRQ: _____

7. הכנס תקליטון שניתן לאתחול עם FDISK.COM ו-SYS.COM או FORMAT.COM לכונן תקליטונים והפעל את המחשב כדי לבצע אתחול מתקליטון ה-DOS.

8. הפעל את FDISK ומחק מציאות קיימות בהתקן USB flash media. צור מחיצה חדשה וסמן אותה כפעילה. צא מ-FDISK על-ידי הקשה על מקש **Esc**.

9. אם לא מתבצעת הפעלה מחדש של המערכת לאחר יציאה מ-FDISK, הקש **Del+Alt+Ctrl** כדי לבצע אתחול מתקליטון DOS.
10. בשורת הפקודה **A:\>FORMAT C: /S** ולאחר מכן הקש **Enter**. התוכנית **FORMAT** תפרמט את התקן **USB flash media**, תוסיף את קובצי המערכת ותבקש תווית לאמצעי האחסון.
11. הקש **Enter** אם אינך מעוניין בתווית, או הזן תווית אם רצונך בכך.
12. כבה את המחשב ונתק את כבל המתח. פתח את המחשב והתקן מחדש את כרטיסי **PCI** שהוצאת לפני כן. סגור את כיסוי המחשב.
13. חבר את כבל המתח, הוצא את התקליטון והפעל את המחשב.
14. עם הפעלת המחשב, הקש **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי להיכנס לתוכנית השירות **Computer Setup**. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.
15. עבור אל **Advanced** (מתקדם) < **PCI Devices** (התקני **PCI**) והפעל מחדש את בקרי **PATA** ו-**SATA** שהשבתת בשלב 6. הקצה לבקר **SATA** את ה-**IRQ** המקורי שלו.
16. שמור שינויים וצא. המחשב יבצע אתחול מהתקן **USB flash media** ככונן **C**.
-
- הערה:**  סדר האתחול המוגדר כברירת מחדל משתנה ממחשב למחשב, וניתן לשנותו בתוכנית השירות **Computer Setup (F10)** (הגדרות המחשב). עיין בתוכנית השירות **Computer Setup (F10)** (הגדרות המחשב) לקבלת הוראות.
- אם השתמשת בגרסת **DOS** מתוך **Windows 9x**, ייתן שתראה את מסך הסמל של **Windows** למשך זמן קצר. אם אינך רואה מסך זה, הוסף קובץ באורך אפס בשם **LOGO.SYS** לספריית השורש של התקן **USB flash media**.
-

חזור לסעיף [העתקה למספר מחשבים בעמוד 18](#).

כאשר Advanced Configuration and Power Interface (ACPI) מופעל, לחצן ההפעלה יכול לפעול הן כלחצן הפעלה/כיבוי והן כלחצן המתנה. מאפיין ההמתנה אינו מנתק לחלוטין את המתח מהמחשב, אלא מעביר את המחשב למצב המתנה עם צריכת מתח נמוכה. מאפיין זה מאפשר לך להוריד במהירות את צריכת המתח ללא סגירת היישומים, ולחזור במהירות למצב הפעלה רגיל מבלי לאבד נתונים.

כדי לשנות את תצורת לחצן ההפעלה, פעל בהתאם לשלבים הבאים:

1. לחץ לחיצה שמאלית על **לחצן Start** (התחל) ולאחר מכן בחר **Control Panel** (לוח הבקרה) < **Power Options** (אפשרויות צריכת חשמל).

2. בחלון **Power Options Properties** (מאפייני אפשרויות צריכת חשמל), לחץ על הכרטיסייה **Advanced** (מתקדם).

3. במקטע **Power Button** (לחצני צריכת חשמל) בחר באפשרות **Standby** (המתנה).

לאחר שלחצן ההפעלה מוגדר לתפקד כלחצן המתנה, לחץ על לחצן ההפעלה כדי להעביר את המערכת למצב צריכת המתח הנמוכה ביותר (מצב המתנה). לחץ שוב על הלחצן כדי להחזיר את המערכת במהירות ממצב המתנה למצב פעולה מלא. כדי לנתק לחלוטין את המתח מהמערכת, לחץ על לחצן ההפעלה ברציפות במשך 4 שניות.

⚠ זיהרות: אין להשתמש בלחצן ההפעלה לכיבוי המחשב, אלא אם כן המערכת אינה מגיבה. כיבוי המחשב ללא התערבות מערכת ההפעלה עלול לגרום לנזק או לאובדן נתונים בכונן הקשיח.

מהנדסי HP מבצעים בדיקות וניפוי שגיאות קפדני לכל תוכנה של HP ושל ספקי צד שלישי, ומפתחים תוכנות תמיכה מיוחדות למערכת ההפעלה כדי להבטיח רמה מיטבית של ביצועים, תאימות ואמינות למחשבים תוצרת HP.

כשעוברים למערכת הפעלה חדשה או משופרת, חשוב להשתמש בתוכנת התמיכה שפותחה למערכת הפעלה זו. אם אתה מתכנן להריץ גרסה של Microsoft Windows השונה מהגרסה המותקנת במחשב, עליך להתקין מנהלי התקן להתקנים וכלי עזר מתאימים, כדי להבטיח תמיכה ותפקוד הולם של כל המאפיינים הנתמכים.

חברת HP הקלה על משימות האיתור, הגישה, ההערכה וההתקנה של תוכנת התמיכה החדשה. באפשרותך להוריד את התוכנה בכתובת <http://www.hp.com/support>.

אתר האינטרנט כולל מנהלי התקן להתקנים, כלי עזר ותמונות זיכרון Flash עדכניים, הדרושים לצורך הפעלת גרסת Microsoft Windows המתקדמת ביותר במחשב HP שברשותך.

10 סטנדרטים מקובלים בשוק

פתרונות הניהול של HP משתלבים עם יישומי ניהול של מערכות אחרות, המבוססים על סטנדרטים מקובלים בשוק, כגון:

- (WBEM) Web-Based Enterprise Management

- (WMI) Windows Management Interface

- Wake on LAN Technology

- ACPI

- SMBIOS

- תמיכה ב-Pre-boot Execution (PXE)

מאפייני בקרת נכסים הנכללים במחשב מספקים נתוני בקרת נכסים חיוניים שניתן לנהלם באמצעות HP Systems Insight Manager, HP Client Configuration Manager, HP Configuration Management Solution, HP Client Manager, או יישומי ניהול מערכת אחרים. שילוב אוטומטי וחלק בין מאפייני בקרת הנכסים ומוצרים אלה מאפשר לך לבחור את כלי הניהול המתאים ביותר לסביבת העבודה, ולמנף את ההשקעה שבוצעה בכלים הקיימים.

כמו כן, HP מציעה מספר פתרונות לבקרת גישה לרכיבים ומידע חשובים במחשב. כאשר HP Embedded Security for ProtectTools מותקן, הוא מונע גישה לא מורשית לנתונים, בודק את תקינות המערכת ומבצע אימות של משתמשי שלישי המנסים לבצע גישה למערכת. (למידע נוסף, עיין במדריך *HP ProtectTools Security Manager Guide* בכתובת <http://www.hp.com/products/security>). תכונות אבטחה כגון HP Embedded Security עבור ProtectTools, ה-Smart Cover Sensor וה-Smart Cover Lock, שזמינות בדגמים מסוימים, מסייעות למנוע גישה לא מורשית לרכיבים פנימיים במחשב האישי. באמצעות השבתת חיבורים מקביליים, טוריים או חיבורי USB, או באמצעות השבתת יכולת אתחול אמצעי אחסון נשלפים, ניתן לספק הגנה לנתונים חשובים. את ההתראות על שינויי זיכרון והתראות ה-Smart Cover Sensor ניתן להעביר אוטומטית הלאה ליישומי ניהול מערכת במטרה למסור הודעות מוקדמות על ניסיונות חדירה למרכיבים הפנימיים של המחשב.

הערה: המאפיינים HP Embedded Security for ProtectTools, Smart Cover Sensor (חיישן הכיסוי החכם) ו-Smart Cover Lock (מנעול הכיסוי החכם) זמינים כרכיבים אופציונליים במערכות מסוימות.

השתמש בתוכניות השירות הבאות כדי לנהל את הגדרות האבטחה במחשב HP:

- באופן מקומי, באמצעות שימוש בתוכנית השירות Computer Setup (הגדרות המחשב). עיין במדריך *תוכנית השירות Computer Setup (הגדרות המחשב) (F10)* המצורף למחשב, לקבלת מידע והוראות נוספות לגבי שימוש בתוכניות השירות להגדרת המחשב. כמו כן, במחשבים מסוימים קיים הרכיב HP BIOS Configuration for ProtectTools, שהנו רכיב מבוסס-Windows של ProtectTools המאפשר למנהלי מערכות לקבוע הגדרות אבטחה של BIOS מתוך מערכת ההפעלה שבשימוש.
 - מרחוק, באמצעות HP Client Manager מ-Symantec, HP Client Automation או System Software Manager. תוכנה זו מאפשרת פריסה ובקרה באופן מאובטח ועקבי של הגדרות האבטחה.
- הטבלה והסעיפים הבאים מתייחסים לניהול מקומי של מאפייני האבטחה של המחשב באמצעות שימוש בתוכנית השירות Computer Setup (הגדרות המחשב) (F10).

טבלה 11-1 מבט כללי על מאפייני אבטחה

אפשרות	תיאור
Setup Password (סיסמת הגדרות)	להגדרה ולהפעלה של סיסמת הגדרות (סיסמת מנהל מערכת). הערה: אם הוגדרה סיסמה, היא נדרשת כדי לשנות אפשרויות בכלי העזר Computer Setup (הגדרות המחשב), לבצע הבזק זיכרון ולערוך שינויים בהגדרות הכנס-הפעל מסוימות בסביבת Windows.
Power-On Password (סיסמת הפעלה)	להגדרה ולהפעלה של סיסמת הפעלה. מופיעה הנחיה בנוגע לסיסמת ההפעלה לאחר כיבוי והפעלה של המחשב. אם המשתמש לא מזין את סיסמת ההפעלה הנכונה, היחידה לא תבצע אתחול.
	הערה: סיסמה זו לא מופיעה במהלך אתחולים חמים, כגון Ctrl+Alt+Delete או Restart from Windows (הפעלה מחדש מתוך Windows), אלא אם כן היא הופעלה תחת Password Options (אפשרויות סיסמה) (ראה להלן).

אפשרות לביצוע הפעולות הבאות:	Password Options (אפשרויות סיסמה)
<ul style="list-style-type: none"> ● נעילת משאבים ישנים (אפשרות זו מופיעה אם מוגדרת סיסמת הגדרות) ● הפעלה/השבתה של מצב שרת רשת (אפשרות זו מופיעה אם מוגדרת סיסמת הפעלה) ● ציון אם הסיסמה דרושה לביצוע אתחול חם (Ctrl+Alt+Delete) (אפשרות זו מופיעה אם מוגדרת סיסמת הפעלה) 	<p>(אפשרות זו תופיע רק אם הוגדרו סיסמת הפעלה או סיסמת הגדרות).</p>
<ul style="list-style-type: none"> ● הפעלה או השבתה של Setup Browse Mode (מצב סקירת הגדרות) (אפשרות זו מופיעה אם הוגדרה סיסמת הגדרות) (מאפשרת הצגה, אך לא שינוי, של F10 Setup Options (אפשרויות של הגדרות F10) מבלי להזין את סיסמת ההגדרות) 	
<ul style="list-style-type: none"> ● הפעלה/השבתה של סיסמה קפדנית (מופיעה אם הוגדרה סיסמת הפעלה), אשר לאחר הפעלתה עוקפת את מגשר הסיסמאות שבמערכת כדי להשבית את סיסמת הפעלה. 	
<p>עייין במדריך לניהול מחשב שולחני לקבלת מידע נוסף.</p>	
אפשרות לביצוע הפעולות הבאות:	Smart Cover (כיסוי חכם) (בדגמים מסוימים)
<ul style="list-style-type: none"> ● נעילה/שחרור של ה-Cover Lock (מנעול הכיסוי). 	
<ul style="list-style-type: none"> ● הגדרת ה-Cover Removal Sensor (חיישן הסרת הכיסוי) לאחת מהאפשרויות הבאות: Disable/Notify User/Setup Password (השבתה/הודעה של סיסמת משתמש/הגדרות). 	
<p>הערה: Notify User (הודעה למשתמש) מתריעה בפני המשתמש כי החיישן גילה שהכיסוי הוסר ממקומו. האפשרות Setup Password (סיסמת הגדרות) מחייבת להזין את סיסמת ההגדרות כדי לבצע אתחול של המחשב במקרה שהחיישן מגלה שהכיסוי הוסר ממקומו.</p>	
<p>תכונה זו נתמכת בדגמים מסוימים בלבד.</p>	
להגדרת האפשרות Device Available/Device Hidden (התקן זמין/התקן נסתר) עבור:	Device Security (אבטחת התקנים)
<ul style="list-style-type: none"> ● יציאות טוריות 	
<ul style="list-style-type: none"> ● יציאה מקבילית 	
<ul style="list-style-type: none"> ● יציאות USB אחריות 	
<ul style="list-style-type: none"> ● יציאות USB קדמיות 	
<ul style="list-style-type: none"> ● יציאות USB פנימיות 	
<ul style="list-style-type: none"> ● שמע מערכת 	
<ul style="list-style-type: none"> ● בקרי רשת (בדגמים מסוימים) 	
<ul style="list-style-type: none"> ● תקליטון ישן 	
<ul style="list-style-type: none"> ● התקן אבטחה משובצת (בדגמים מסוימים) 	
<ul style="list-style-type: none"> ● SATA0 	
<ul style="list-style-type: none"> ● SATA1 (בדגמים מסוימים) 	
<ul style="list-style-type: none"> ● SATA2 (בדגמים מסוימים) 	
<ul style="list-style-type: none"> ● SATA3 (בדגמים מסוימים) 	
<ul style="list-style-type: none"> ● eSATA (בדגמים מסוימים) 	
להפעלה/השבתה של יכולת המחשב לבצע אתחול ממערכת הפעלה המותקנת בשרת הרשת. (מאפיין זה קיים בדגמי NIC בלבד; על בקר הרשת להיות כרטיס הרחבה מסוג PCI או שעליו להיות משובץ בלוח המערכת).	Network Service Boot (אתחול שירות רשת)

להגדרה של:	System Ids (זיהוי המערכת)
<ul style="list-style-type: none"> • תווי נכס (זיהוי של 18 בתים), מספר זיהוי נכס שהקצתה החברה למחשב. • תווי בעלות (זיהוי של 80 בתים) מוצגת במהלך הבדיקה העצמית של המחשב. • מספר סידורי של המארז או מספר זיהוי אוניברסלי ייחודי (UUID). ניתן לעדכן את UUID רק אם המספר הסידורי הנוכחי של המארז אינו תקף. (מספרי זיהוי אלה נקבעים בדרך-כלל על-ידי היצרן והם משמשים לזיהוי חד משמעי של המערכת). • הגדרות מקולדת מקומיות (לדוגמה, אנגלית או גרמנית) לצורך הכנסת זיהוי המערכת. 	
<p>להקצאה או לשינוי סיסמת מנהל מערכת או סיסמת משתמש עבור כוננים קשיחים. כשמאפיין זה מופעל, המשתמש מתבקש להזין את אחת מסימאות DriveLock במהלך הבדיקה העצמית של המחשב. אם אף סיסמה לא הוזנה בהצלחה, הכונן הקשיח לא יהיה נגיש עד להזנת אחת הסימאות בהצלחה במהלך רצף האתחול הקר.</p> <p>הערה: בחירה זו תופיע אך ורק במקרה שבו לפחות כונן אחד התומך בתכונת DriveLock, מחובר למערכת.</p>	DriveLock Security (אבטחת DriveLock)
<p>Data Execution Prevention (מניעת הפעלת נתונים) (בדגמים מסוימים) (הפעלה/השבתה) - אפשרות זו מסייעת למנוע פרוצות אבטחה במערכת ההפעלה.</p> <p>Virtualization Technology (טכנולוגיית הדמיה) (בדגמים מסוימים) (הפעלה/השבתה) - אפשרות זו שולטת במאפייני ההדמיה של המעבד. שינוי הגדרה זו מחייב כיבוי של המחשב והפעלתו מחדש.</p> <p>Virtualization Technology Directed I/O (קלט/פלט המנוהל על-ידי טכנולוגיית הדמיה) (בדגמים מסוימים) (הפעלה/השבתה) - אפשרות זו שולטת במאפייני היסודיים של המעבד ושל מערך השבבים הדרושים לצורך תמיכה בכלי וירטואלי. שינוי הגדרה זו מחייב כיבוי של המחשב והפעלתו מחדש. כדי להפעיל מאפיין זה עליך להפעיל את המאפיינים הבאים:</p> <p>Trusted Execution Technology (טכנולוגיית הפעלה אמינה) (בדגמים מסוימים) (הפעלה/השבתה) - אפשרות זו שולטת במאפיינים היסודיים של המעבד ושל מערך השבבים הדרושים לצורך תמיכה בכלי וירטואלי. שינוי הגדרה זו מחייב כיבוי של המחשב והפעלתו מחדש. כדי להפעיל מאפיין זה עליך להפעיל את המאפיינים הבאים:</p> <ul style="list-style-type: none"> • Embedded Security Device Support (תמיכה בהתקן האבטחה המשובצת) • Virtualization Technology (טכנולוגיית הדמיה) • Virtualization Technology Directed I/O (קלט/פלט המנוהל על-ידי טכנולוגיית הדמיה) <p>Embedded Security Device Support (תמיכה בהתקן האבטחה המשובץ) (בדגמים מסוימים) (הפעלה/השבתה) - אפשרות זו מתירה הפעלה והשבתה של התקן האבטחה המשובץ. שינוי הגדרה זו מחייב כיבוי של המחשב והפעלתו מחדש.</p> <p>הערה: כדי להגדיר את תצורת ה-Embedded Security Device (התקן האבטחה המשובצת), יש להגדיר סיסמת Setup (הגדרות).</p>	System Security (אבטחת מערכת) (בדגמים מסוימים: אפשרויות אלה תלויות בחומרה)
<ul style="list-style-type: none"> • Reset to Factory Settings (איפוס להגדרות היצרן) (בדגמים מסוימים) Do not reset/Reset (אל תאפס/אפס) - איפוס להגדרות ברירת המחדל של היצרן ימחק את כל סיסמאות האבטחה. שינוי הגדרה זו מחייב כיבוי של המחשב והפעלתו מחדש. <p>זהירות: התקן האבטחה המשובצת הוא רכיב חיוני בסכימות אבטחה רבות. מחיקה של סיסמאות האבטחה תמנע גישה לנתונים המוגנים על-ידי ה-Embedded Security Device (התקן האבטחה המשובצת). בחירה ב-Reset to Factory Settings (איפוס להגדרות היצרן) עלולה לגרום לאובדן נתונים ניכר.</p> <ul style="list-style-type: none"> • Power-on authentication support (תמיכה באימות בהפעלה) (בדגמים מסוימים) (הפעלה/השבתה) - אפשרות זו שולטת בסכימת האימות של סיסמת ההפעלה שעושה שימוש בהתקן האבטחה המשובץ. שינוי הגדרה זו מחייב כיבוי של המחשב והפעלתו מחדש. • Reset authentication credentials (איפוס המלצה לאימות) (בדגמים מסוימים) Do not reset/Reset (אל תאפס/אפס) - הבחירה ב-Reset (אפס) משביתה את התמיכה באימות ומוחקת את פרטי האימות מהתקן האבטחה המשובץ. שינוי הגדרה זו מחייב כיבוי של המחשב והפעלתו מחדש. <p>OS management of Embedded Security Device (ניהול התקן האבטחה המשובץ על-ידי מערכת ההפעלה) (בדגמים מסוימים) (הפעלה/השבתה) - אפשרות זו מאפשרת למשתמש להגביל את השליטה של מערכת ההפעלה</p>	

בהתקן האבטחה המשובץ. שינוי הגדרה זו מחייב כיבוי של המחשב והפעלתו מחדש. אפשרות זו מאפשרת למשתמש להגביל את השליטה של מערכת ההפעלה בהתקן האבטחה המשובץ.

- **Reset of Embedded Security Device through OS** (איפוס של התקן האבטחה המשובץ באמצעות מערכת ההפעלה) (בדגמים מסוימים) (הפעלה/השבתה) - אפשרות זו מאפשרת למשתמש להגביל את יכולת מערכת ההפעלה לדרוש **Reset to Factory Settings** (איפוס להגדרות היצרן) של התקן האבטחה המשובץ. שינוי הגדרה זו מחייב כיבוי של המחשב והפעלתו מחדש.

הערה: כדי להפעיל אפשרות זו, יש להגדיר סיסמת Setup (הגדרות).

Smart Card BIOS Password Support (תמיכה בסיסמת BIOS של כרטיס חכם) (בדגמים מסוימים) (הפעלה/השבתה) - אפשרות זו מאפשרת למשתמש להפעיל/להשבית את הכרטיס החכם כך שישמש במקום סיסמאות ההגדרות וההפעלה. הגדרה זו דורשת אתחול נוסף ב-ProtectTools לפני שהיא תיכנס לתוקף.

PAVP (בדגמים מסוימים) (השבתה/מינימום/מקסימום) - האפשרות **PAVP** מפעילה את **Protected Audio Video** (נתיב מוגן של שמע ווידאו) במערך השבבים. אפשרות זו עשויה לאפשר הצגה של תוכן מוגן מסוים בחדות גבוהה שבמקרים אחרים יהיה אסור להפעלה. בחירה באפשרות המקסימום תקצה 96 MB של זיכרון מערכת ל-PAVP באופן בלעדי.

Setup Security Level (רמת האבטחה של ההגדרות)

שיטה המאפשרת למשתמש-קצה גישה מוגבלת לשינוי אפשרויות מסימות של ההגדרות, מבלי שיצטרכו לדעת את סיסמת ההגדרות.

מאפיין זה מספק למנהל המערכת גמישות בהגנה על שינויים שבוצעו באפשרויות חיוניות של ההגדרות, ובו בזמן מאפשר למשתמש להציג את הגדרות המערכת ולהגדיר אפשרויות לא חיוניות. מנהל המערכת קובע את זכויות הגישה לאפשרויות מסימות של ההגדרות בהתאם למקרה הנתון, באמצעות התפריט **Setup Security Level** (רמת האבטחה של ההגדרות). כברירת מחדל, לכל האפשרויות של ההגדרות מוקצית **Setup Password** (סימת הגדרות), וכדי לבצע שינויים באחת מהאפשרויות המשתמש חייב להזין את סיסמת ההגדרות הנכונה במהלך הבדיקה העצמית של המחשב. המנהל יכול להגדיר פריטים מסוימים ל-None (ללא), ובמצב זה המשתמש יכול לבצע שינויים באפשרויות שצוינו אם נעשה ניסיון לגשת להגדרות באמצעות סיסמאות שגויות. האפשרות **None** (ללא) מוחלפת בסימת הפעלה (**Power-On Password**) אם מופעלת סיסמת הפעלה.

הערה: יש להגדיר את האפשרות **Setup Browse Mode** (מצב סקירת הגדרות) ל-**Enable** (הפעלה) על מנת שהמשתמש יוכל להיכנס ל-Setup (הגדרות) מבלי לדעת את סיסמת ההגדרות.

אבטחה באמצעות סיסמה

סימת ההפעלה מונעת שימוש לא-חוקי במחשב בכך שהיא דורשת הזנת סיסמה לצורך גישה ליישומים או נתונים בכל פעם שמפעילים או מבצעים אתחול מחדש של המחשב. סיסמת ההגדרות מיועדת במיוחד למניעת גישה לא-חוקית להגדרות מערכת, וניתן להשתמש בה כדי לדרוס את סיסמת ההפעלה. כלומר, במקרה שנדרשים להזין סיסמת הפעלה, ניתן להזין במקום זאת את סיסמת ההגדרות, וכך תתאפשר גישה למחשב.

ניתן להגדיר סיסמת הגדרות לכל הרשת כדי לאפשר למנהל הרשת להתחבר לכל המחשבים ברשת לצורכי תחזוקה, מבלי שיצטרך לדעת את סיסמאות ההפעלה שלהם, גם אם הוגדרו כאלה.

קביעת סיסמת הגדרות באמצעות Computer Setup (הגדרות המחשב)

אם במערכת מותקן התקן אבטחה משובץ, עיין ב-**HP ProtectTools Security Manager Guide** (מדריך למנהל האבטחה **HP ProtectTools**), בכתובת <http://www.hp.com>. יצירת סיסמת הגדרות באמצעות **Computer Setup** (הגדרות המחשב) מונעת ביצוע שינויים בתצורת המחשב (שימוש בתוכנית השירות **Computer Setup** (הגדרות המחשב) (F10)) עד להזנת הסיסמה.

1. הפעל או הפעל מחדש את המחשב. אם אתה נמצא ב-Windows, לחץ על **Start** (התחל) < **Shut Down** (כיבוי) < **Restart** (הפעלה מחדש).
2. עם הפעלת המחשב, הקש **F10** לפני שהמחשב מתחיל למערכת ההפעלה כדי להיכנס לתוכנית השירות **Computer Setup**. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.

הערה: אם לא הקשת **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב ולהקיש שוב על **F10** לפני שהמחשב מתחיל למערכת ההפעלה כדי לגשת לתוכנית השירות.

3. בחר באפשרות **Security** (אבטחה), ולאחר מכן בחר באפשרות **Setup Password** (סימת הגדרות) ופעל בהתאם להוראות שעל-גבי המסך.

4. לסיום, לחץ על **File** (קובץ) < **Save Changes and Exit** (שמירת שינויים ויציאה).

קביעת סימת הפעלה (Power-On) באמצעות Computer Setup (הגדרות המחשב)

קביעת סימת הפעלה באמצעות Computer Setup מונעת גישה למחשב לאחר הפעלתו, כל עוד לא הוזנה סימה. לאחר הגדרת סימת הפעלה, Computer Setup מציג את ה-**Password Options** (אפשרויות סימה) בתפריט **Security** (אבטחה). אפשרויות הסימה כוללות את **Password Prompt on Warm Boot** (בקשה להזנת סימה באתחול חם). כאשר האפשרות **Password Prompt on Warm Boot** (בקשה להזנת סימה באתחול חם) מופעלת, יש להזין גם את הסימה בכל פעם שהמחשב מופעל מחדש.

1. הפעל או הפעל מחדש את המחשב. אם אתה נמצא ב-Windows, לחץ על **Start** (התחל) < **Shut Down** (כיבוי) < **Restart** (הפעלה מחדש).

2. עם הפעלת המחשב, הקש **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי להיכנס לתוכנית השירות Computer Setup. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.

הערה: אם לא הקשת **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב ולהקיש שוב על **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי לגשת לתוכנית השירות.

3. בחר בתפריט **Security** (אבטחה) ולאחר מכן בחר **Power-On Password** (סימת הפעלה) ופעל בהתאם להוראות שעל-גבי המסך.

4. לסיום, לחץ על **File** (קובץ) < **Save Changes and Exit** (שמירת שינויים ויציאה).

הזנת סימת הפעלה

כדי להזין סימת הפעלה, בצע את השלבים הבאים:

1. הפעל או הפעל מחדש את המחשב. במערכת ההפעלה Windows, לחץ על **Start** (התחל) < **Shut Down** (כיבוי) < **Restart the Computer** (הפעלה מחדש של המחשב).

2. לאחר שסמל המפתח מופיע על-גבי הצג, הקלד את הסימה הנוכחית ולאחר מכן הקש **Enter**.

הערה: הקלד בזהירות; מטעמי אבטחה, התווים המוקלדים אינם מוצגים על המסך.

אם טעית בהקלדת הסימה, יופיע סמל של מפתח שבור. נסה שנית. לאחר שלושה ניסיונות כושלים, יהיה עליך לכבות את המחשב ולהפעילו מחדש לפני שתוכל להמשיך.

הזנת סימת הגדרות

אם במערכת מותקן התקן אבטחה משובץ, עיין ב-*HP ProtectTools Security Manager Guide* (מדריך למהל האבטחה *HP ProtectTools*), בכתובת <http://www.hp.com>.

אם הוגדרה סימת הגדרות במחשב, תתבקש להזין סימה זו בכל פעם שבה תפעיל את הגדרות המחשב.

1. הפעל או הפעל מחדש את המחשב. אם אתה נמצא ב-Windows, לחץ על **Start** (התחל) < **Shut Down** (כיבוי) < **Restart** (הפעלה מחדש).

2. עם הפעלת המחשב, הקש **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי להיכנס לתוכנית השירות Computer Setup. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.

הערה: אם לא הקשת **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב ולהקיש שוב על **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי לגשת לתוכנית השירות.

3. לאחר שסמל המפתח מופיע על-גבי הצג, הקלד את סימת ההגדרות הנוכחית ולאחר מכן הקש **Enter**.

הערה: הקלד בזהירות; מטעמי אבטחה, התווים המוקלדים אינם מוצגים על המסך.

אם טעית בהקלדת הסיסמה, יופיע סמל של מפתח שבור. נסה שנית. לאחר שלושה ניסיונות כושלים, יהיה עליך לכבות את המחשב ולהפעילו מחדש לפני שתוכל להמשיך.

שינוי סיסמת הפעלה או סיסמת הגדרות

אם במערכת מותקן התקן אבטחה משובץ, עיין ב-*HP ProtectTools Security Manager Guide* (מדריך למנהל האבטחה *HP ProtectTools*, בכתובת <http://www.hp.com>).

1. הפעל או הפעל מחדש את המחשב. במערכת ההפעלה Windows, לחץ על **Start** (התחל) < **Shut Down** (כיבוי) < **Restart the Computer** (הפעלה מחדש של המחשב).

2. כדי להחליף את סיסמת ההפעלה, עבור לשלב 3.

כדי לשנות את סיסמת ההגדרות, עם הפעלת המחשב, הקש **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי להיכנס לתוכנית השירות *Computer Setup*. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.

הערה: אם לא הקשת **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב ולהקיש שוב על **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי לגשת לתוכנית השירות.

3. לאחר הופעת סמל המפתח, הקלד את הסיסמה הנוכחית, קו נטוי (/) או תו הפרדה חלופי, סיסמה חדשה, קו נטוי (/) או תו הפרדה חלופי, והסיסמה החדשה שנית, לפי הדוגמה הבאה: סיסמה נוכחית/סיסמה חדשה/סיסמה חדשה

הערה: הקלד בזהירות; מטעמי אבטחה, התווים המוקלדים אינם מוצגים על המסך.

4. הקש **Enter**.

בפעם הבאה שתפעיל את המחשב, הסיסמה החדשה תיכנס לתוקף.

הערה: לקבלת מידע נוסף אודות תווי ההפרדה החלופיים, עיין בסעיף [תווי הפרדה במקלדות של שפות שונות](#) **בעמוד 31**. ניתן לשנות את סיסמת ההפעלה וסימת ההגדרות על-ידי שימוש באפשרויות האבטחה ב-*Computer Setup* (הגדרות המחשב).

מחיקת סיסמת הפעלה או סיסמת הגדרות

אם במערכת מותקן התקן אבטחה משובץ, עיין ב-*HP ProtectTools Security Manager Guide* (מדריך למנהל האבטחה *HP ProtectTools*, בכתובת <http://www.hp.com>).

1. הפעל או הפעל מחדש את המחשב. במערכת ההפעלה Windows, לחץ על **Start** (התחל) < **Shut Down** (כיבוי) < **Restart the Computer** (הפעלה מחדש של המחשב).

2. כדי למחוק את סיסמת ההפעלה, עבור לשלב 3.

כדי למחוק את סיסמת ההגדרות, עם הפעלת המחשב, הקש **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי להיכנס לתוכנית השירות *Computer Setup*. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.

הערה: אם לא הקשת **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב ולהקיש שוב על **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי לגשת לתוכנית השירות.

3. לאחר הופעת סמל המפתח, הקלד את הסיסמה הנוכחית שלך ואחריה קו נטוי (/) או תו הפרדה חלופי לפי הדוגמה הבאה: סיסמה נוכחית/

4. הקש **Enter**.



הערה: לקבלת מידע נוסף אודות תווי הפרדה החלופיים, עיין בסעיף **תווי הפרדה במקלדות של שפות שונות** **בעמוד 31**. ניתן לשנות את סיסמת ההפעלה וסימת ההגדרות על-ידי שימוש באפשרויות האבטחה ב-Computer Setup (הגדרות המחשב).

תווי הפרדה במקלדות של שפות שונות

כל מקלדת מתוכננת כך שתתאים לדרישות המיוחדות של כל מדינה/אזור. התחביר והמקשים שבהם תשתמש לשינוי או למחיקת הסיסמה, תלויים במקלדת שסופקה עם המחשב שלך.

תווי הפרדה במקלדות של שפות שונות

/	ערבית	-	יוונית	/	רוסית
=	בלגית	.	עברית	-	סלובקית
-	*BHCMSS	-	הונגרית	-	ספרדית
/	ברזילאית	-	איטלקית	/	שוודית/פינית
/	סינית	/	יפנית	-	שוויצרית
-	צ'כית	/	קוריאנית	/	טיוואנית
-	דנית	-	אמריקה לטינית	/	תאילנדית
!	צרפתית	-	נורווגית	.	טורקית
é	צרפתית קנדית	-	פולנית	/	אנגלית (ארה"ב)
-	גרמנית	-	פורטוגזית		

* עבור בוסניה-הרצגובינה, מונטנגרו, סלובניה, סרביה וקראטיה.

ביטול סיסמאות

אם שכחת את הסיסמה, לא תוכל להפעיל את המחשב. עיין במדריך לפתרון בעיות לקבלת הוראות אודות ביטול סיסמאות.

אם במערכת מותקן התקן אבטחה משובץ, עיין ב-*HP ProtectTools Security Manager Guide* (מדריך למנהל האבטחה *HP ProtectTools*, בכתובת <http://www.hp.com>).

DriveLock

DriveLock הוא מאפיין אבטחה מקובל בתעשייה המונע גישה לא-חוקית לנתונים בכונן קשיח מסוג ATA. DriveLock מיושם כהרחבה ל-Computer Setup (הגדרות המחשב). מאפיין זה זמין רק כאשר כוננים קשיחים התומכים בקבוצת פקודות האבטחה של ATA מזהים. DriveLock מיועד ללקוחות HP שמייחסים חשיבות רבה לנושא אבטחת הנתונים. ללקוחות כאלה, עלות של כונן קשיח היא זניחה בהשוואה לנזק העלול לבבוע מגישה לא-חוקית לתוכן הכונן הקשיח. כדי לאזן בין רמה גבוהה זו של אבטחה לבין הצורך השכיח לקבלת סיסמה שנשכחה, DriveLock מפעיל סכימת אבטחה בעלת שתי סיסמאות. סיסמה אחת מיועדת לשמש את מנהל המערכת, ואילו הסיסמה השנייה משמשת בדרך כלל את משתמש הקצה. אין שום דרך לשחרור הכונן אם שתי הסיסמאות אובדות. לכן, השימוש ב-DriveLock הוא הבטוח ביותר כשנתונים הנמצאים בכונן הקשיח מועתקים במערכת מידע שיתופית, או כשהם מגויבים באופן סדיר. במקרה ששתי סיסמאות DriveLock נשכחו, לא ניתן יהיה להשתמש בכונן הקשיח. לגבי משתמשים שאינם מתאימים לפרופיל הלקוחות המוגדר, הדבר עלול לגרום סיכון חמור. לגבי משתמשים המתאימים לפרופיל הלקוחות, הסיכון הוא סביר בהתחשב באופי הנתונים השמורים בכונן הקשיח.

שימוש ב- DriveLock

כאשר אחד או יותר מהכוננים הקשיחים שתומכים בסדרת הפקודות ATA Security מזהים, האפשרות DriveLock מופיעה תחת תפריט Security (אבטחה) ב-Computer Setup (הגדרות המחשב). למשתמש מוצגת אפשרות להגדיר סיסמת מנהל מערכת או להפעיל את DriveLock. יש להזין את סיסמת המשתמש כדי להפעיל את DriveLock. מכיוון שהגדרת התצורה הראשונית של DriveLock מבוצעת בדרך כלל על ידי מנהל המערכת, יש להגדיר תחילה סיסמת מנהל מערכת. HP מעודדת את מנהלי המערכת להגדיר סיסמת מנהל מערכת גם כשבכוננתם להפעיל את DriveLock, וגם כשבכוננתם להשבית את פעולתו. הדבר יספק למנהל המערכת יכולת לשנות את הגדרות DriveLock במקרה שהכונן יינעל בעתיד. לאחר הגדרת סיסמת מנהל מערכת יכול מנהל המערכת להחליט אם להפעיל את DriveLock או להמשיך להשבית אותו.

אם נמצא כונן קשיח נעול, הבדיקה העצמית של המחשב תדרוש סיסמה כדי לשחרר את ההתקן. אם הוגדרה סיסמת הפעלה, והיא תואמת את סיסמת המשתמש של ההתקן, הבדיקה העצמית של המחשב לא תדרוש מהמשתמש להזין מחדש את הסיסמה. אחרת, יידרש המשתמש להזין סיסמת DriveLock. באתחול קר, ניתן להשתמש הן בסיסמת מנהל המערכת והן בסיסמת המשתמש. באתחול חם, הזן את אותה הסיסמה המשתמשת לשחרור הכונן במהלך האתחול הקר שקדם לו. למשתמשים יינתנו שני ניסיונות להזין את הסיסמה הנכונה. באתחול קר, אם שני הניסיונות ייכשלו, הבדיקה העצמית תמשיך להתבצע, אך הנתונים שבכונן לא יהיו זמינים. באתחול חם או בהפעלה מחדש מתוך Windows, אם שני הניסיונות ייכשלו, הבדיקה העצמית תיעצר והמשתמש יתבקש לכבות את המחשב ולהפעיל אותו מחדש.

יישומי DriveLock

השימוש המעשי ביותר במאפיין האבטחה של DriveLock הוא בסביבה ארגונית. מנהל המערכת אחראי להגדיר את תצורת הכונן הקשיח, והדבר מחייב בין השאר להגדיר סיסמת מנהל מערכת של DriveLock וסיסמה זמנית של המשתמש. במקרה שהמשתמש שוכח את סיסמת המשתמש או שהציווד מועבר לעובד אחר, ניתן לעשות שימוש בסיסמת מנהל מערכת כדי להגדיר מחדש את סיסמת המשתמש ולהשיג גישה לכונן הקשיח.

HP ממליצה שמנהלי מערכת ארגוניים שבחרים להפעיל את DriveLock, יגדירו גם מדיניות ארגונית לצורך הגדרה ותחזוקה של סיסמאות מנהלי מערכת. הדבר חייב להתבצע כדי למנוע מצב שבו העובד יפעיל בשגגה או בזדון את שתי סיסמאות DriveLock לפני פרישתו מהחברה. בתרחיש כזה לא ניתן יהיה להשתמש בכונן הקשיח, ויהיה צורך להחליפו. באופן דומה, אם לא תוגדר סיסמת מנהל מערכת, מנהלי המערכת עלולים להיקלע למצב שבו אין להם גישה לכונן הקשיח ואין ביכולתם לבצע בדיקות שגרתיות לתוכנות לא-חוקיות, פונקציות בקרת נכסים נוספות ופעולות תמיכה.

למשתמשים בעלי דרישות אבטחה חמורות פחות, HP אינה ממליצה להפעיל את DriveLock. משתמשים הנמצאים בקטגוריה זו כוללים משתמשים אישיים או משתמשים שאינם מחזיקים מידע יומיומי רגיש בכוננים הקשיחים שלהם. למשתמשים אלה, קריסה אפשרית של הכונן הקשיח כתוצאה משכיחת שתי הסיסמאות חשובה הרבה יותר מערך הנתונים ש-DriveLock נועד לאבטח. ניתן להגביל את הגישה להגדרות מערכת ול-DriveLock באמצעות סיסמת הגדרות. הגדרת סיסמת הגדרות מבלי למוסרה למשתמשי הקצה מאפשרת למנהלי המערכת להגביל את יכולת המשתמשים להפעיל את DriveLock.

Smart Cover Sensor (חיישן הכיסוי החכם)

חיישן הסרת הכיסוי הקיים בחלק מהדגמים הוא צירוף של טכנולוגיות חומרה ותוכנה, המאפשר להציג התרעות במקרה של הסרת כיסוי המחשב או לוח הצד. קיימות שלוש רמות הגנה, כמתואר בטבלה הבאה.

טבלה 11-2 רמות הגנה של ה-Smart Cover Sensor (חיישן הכיסוי החכם)

רמה	הגדרה	תיאור
Level 0 (רמה 0)	Disabled (מושבתת)	Smart Cover Sensor (חיישן הכיסוי החכם) מושבת (ברירת מחדל).
Level 1 (רמה 1)	Notify User (הודעה למשתמש)	כשהמחשב מופעל מחדש, מופיעה על הצג הודעה על כך שכיסוי המחשב או לוח הצד הוסרו.
Level 2 (רמה 2)	Setup Password (סימת הגדרות)	כשהמחשב מופעל מחדש, מופיעה על הצג הודעה על כך שכיסוי המחשב או לוח הצד הוסרו. יש להזין סימת הגדרות כדי להמשיך.

הערה: הגדרות אלה ניתנות לשינוי באמצעות הגדרות המחשב. לקבלת מידע נוסף אודות Computer Setup (הגדרות המחשב), עיין במדריך לתוכנית השירות Computer Setup (הגדרות המחשב) (F10).

הגדרת רמת ההגנה של ה-Smart Cover Sensor (חיישן הכיסוי החכם)

כדי להגדיר את רמת האבטחה של ה-Smart Cover Sensor (חיישן הכיסוי החכם), בצע את השלבים הבאים:

1. הפעל או הפעל מחדש את המחשב. אם אתה נמצא ב-Windows, לחץ על **Start** (התחל) < **Shut Down** (כיבוי) < **Restart** (הפעלה מחדש).
2. עם הפעלת המחשב, הקש **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי להיכנס לתוכנית השירות Computer Setup. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.
- הערה:** אם לא הקשת **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב ולהקיש שוב על **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי לגשת לתוכנית השירות.
3. בחר **Security** (אבטחה) < **Smart Cover** (כיסוי חכם) < **Cover Removal Sensor** (חיישן הסרת הכיסוי), ובחר ברמת האבטחה הרצויה.
4. לסיום, לחץ על **File** (קובץ) < **Save Changes and Exit** (שמירת שינויים ויציאה).

Smart Cover Lock (מנעול הכיסוי החכם)

מנעול הכיסוי החכם הוא מנעול כיסוי הנשלט באמצעות תוכנה, שנכלל בדגמים מסוימים של מחשבי HP. נעילה זו מונעת גישה לא חוקית לרכיבים הפנימיים של המחשב. המחשבים מסופקים כאשר מנעול הכיסוי החכם נמצא במצב לא נעול.

הירות: כדי להגיע לרמת האבטחה המרבית של מנעול הכיסוי החכם, הקפד להגדיר סימת הגדרות. סימת ההגדרות מונעת גישה בלתי מורשית לכלי העזר Computer Setup (הגדרות המחשב).

הערה: ה-Smart Cover Lock (מנעול הכיסוי החכם) זמין כרכיב אופציונלי במערכות מסוימות.

נעילת מנעול הכיסוי החכם

כדי להפעיל ולנעול את מנעול הכיסוי החכם, פעל לפי השלבים הבאים:

1. הפעל או הפעל מחדש את המחשב. אם אתה נמצא ב-Windows, לחץ על **Start** (התחל) < **Shut Down** (כיבוי) < **Restart** (הפעלה מחדש).
 2. עם הפעלת המחשב, הקש **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי להיכנס לתוכנית השירות Computer Setup. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.
-
- הערה:** אם לא הקשת **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב ולהקיש שוב על **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי לגשת לתוכנית השירות.
3. בחר **Security** (אבטחה) < **Smart Cover** (כיסוי חכם) < **Cover Lock** (מנעול הכיסוי) < **Lock option** (אפשרות הנעילה).
 4. לסיום, לחץ על **File** (קובץ) < **Save Changes and Exit** (שמירת שינויים ויציאה).

שחרור מנעול הכיסוי החכם

1. הפעל או הפעל מחדש את המחשב. אם אתה נמצא ב-Windows, לחץ על **Start** (התחל) < **Shut Down** (כיבוי) < **Restart** (הפעלה מחדש).
 2. עם הפעלת המחשב, הקש **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי להיכנס לתוכנית השירות Computer Setup. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.
-
- הערה:** אם לא הקשת **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב ולהקיש שוב על **F10** לפני שהמחשב מאתחל למערכת ההפעלה כדי לגשת לתוכנית השירות.
3. בחר **Security** (אבטחה) < **Smart Cover** (כיסוי חכם) < **Cover Lock** (מנעול הכיסוי) < **Unlock** (שחרור נעילה).
 4. לסיום, לחץ על **File** (קובץ) < **Save Changes and Exit** (שמירת שינויים ויציאה).

שימוש ב-Smart Cover FailSafe Key

אם הפעלת את מנעול הכיסוי החכם, ואינך יכול להזין סיסמה כדי להשבית את המנעול, תצטרך מפתח FailSafe (אל-כשל) ל-Smart Cover (הכיסוי החכם) כדי לפתוח את כיסוי המחשב. יהיה עליך להשתמש במפתח בכל אחד מהמקרים הבאים:

- הפסקת חשמל
- כשל באתחול
- כשל של אחד מרכיבי המחשב (כגון מעבד או ספק מתח)
- סיסמה שנשכחה

זהירות: Smart Cover FailSafe Key הוא כלי ייחודי המסופק על-ידי HP. היה מוכן; הזמן מפתח זה לפני שתזדקק לו אצל משווק או ספק שירות מורשה.

כדי לקבל את מפתח האל-כשל (FailSafe), בצע אחת מהפעולות הבאות:

- פנה למשווק מורשה או לספק שירות מורשה של HP
 - התקשר למספר המופיע בכתב האחריות
- לקבלת מידע נוסף אודות שימוש ב-Smart Cover FailSafe Key (מפתח אל-כשל לכיסוי חכם), עיין במדריך עזר לרכיבי חומרה.

Cable Lock Provision (התקן מנעול כבל)

הלוח האחורי של המחשב (בדגמים מסוימים) כולל מנעול כבל, כך שניתן לאבטח את המחשב פיזית למשטח העבודה. להוראות מלוות באיורים, עיין במדריך עזר לרכיבי חומרה.

טכנולוגיה לזיהוי טביעות אצבע

הטכנולוגיה לזיהוי טביעות אצבע של HP מעלה את רמת האבטחה של הרשת באמצעות ביטול הצורך בהזנת סיסמת משתמש, מפשטת את תהליך ההתחברות לרשת ומצמצמת עלויות ניהול של רשתות שיתופיות. זוהי טכנולוגיה שמחירה סבירים, ואינה מיועדת אך ורק לחברות היי-טק או ארגונים הדורשים רמת אבטחה גבוהה.

הערה: התמיכה בטכנולוגית זיהוי טביעות אצבע משתנה מדגם לדגם.

הודעות כשל והתאוששות

מאפייני דיווח על תקלות והתאוששות משלבים טכנולוגיה חדשנית של חומרה ותוכנה כדי למנוע אובדן של נתונים קריטיים וכדי להקטין ככל שניתן הפסקות עבודה בלתי מתוכננות.

אם המחשב מחובר לרשת המנוהלת על-ידי HP Client Manager, המחשב שולח הודעה על כשל ליישום ניהול הרשת. באמצעות HP Client Manager Software, תוכל גם לתזמן מרחוק כלי אבחון, שיפעלו באופן אוטומטי בכל המחשבים המנוהלים, ויצרו דו"ח סיכום של כל הבדיקות שנשלו.

Drive Protection System (מערכת להגנה על כוננים)

Drive Protection System (DPS), מערכת להגנה על כוננים) היא כלי אבחון הנכלל בכוננים קשיחים המותקנים במחשבים מסוימים של HP. מערכת DPS מיועדת לסייע באבחון תקלות, היכולות לגרום להחלפה בלתי מוצדקת של הכונן הקשיח.

בתהליך ההרכבה של מחשבי HP, כל כונן קשיח המותקן בהם עובר בדיקה באמצעות DPS, ורשומה קבועה עם פרטי המפתח נכתבת בכונן. בכל פעם שמפעילים את DPS, תוצאות הבדיקה מאוחסנות בכונן הקשיח. ספק השירות יכול להיעזר במידע זה לצורך אבחון הנסיבות שגרמו לך להפעיל את תוכנת DPS. עיין במדריך לפתרון בעיות לקבלת הוראות אודות שימוש ב-DPS.

אספקת מתח עמידה בנחשולי מתח

אספקת מתח שעמידה בנחשולי מתח מאפשרת אמינות גבוהה יותר במקרים שבהם המחשב נפגע מנחשול מתח בלתי צפוי. אספקת מתח מסוג זה מתוכננת לעמוד בפני נחשולי מתח של עד 2000V ללא קריסת מערכת או אובדן מידע כלשהו.

חיישן תרמי

חיישן תרמי הוא תכונה המשלבת חומרה ותוכנה, העוקבת אחר הטמפרטורה הפנימית של המחשב. תכונה זו מציגה הודעת זהירות אם חלה חריגה מהתחום הנורמלי, ובכך ניתן לך די זמן לנקוט פעולה לפני שייגרם נזק לרכיבים פנימיים ולפני שיאבדו נתונים.

זהירות: מצב של טמפרטורה גבוהה עלול להוביל לנזק למערכת או לאובדן נתונים.

התקן USB flash media, ניתן לאתחול 18, 20	התקנה ראשונית 2	התקנה מרחוק 4	התקן מנעול כבל 35	התקן שניתן לאתחול USB flash media 18	יצירה 18
ז					
זיכרון הבזק Remote ROM Flash 15	זיכרון הבזק ROM 15				
ח					
חיישן תרמי 35					
ט					
טכנולוגיה לזיהוי טביעות אצבע 35	טכנולוגיית ניהול 12	טמפרטורה פנימית, מחשב 35	טמפרטורה פנימית של המחשב 35		
כ					
כונן, הגנה 35					
כוננים קשיחים, כלי אבחון 35					
כלי אבחון לכוננים קשיחים 35					
כלי פריסה, תוכנה 2					
כלי שכפול, תוכנה 2					
כתובות אינטרנט. ראה אתרי אינטרנט					
ל					
לחצן הפעלה דו-מצבי 22					
מ					
מחיקת סיסמה 30					
מנעול הכיסוי 33					
מערכות הפעלה, תמיכה בהחלפה 23					
א					
אבטחה					
31 DriveLock					
ProtectTools Security Manager 7					
Smart Cover Lock (מנעול הכיסוי החכם) 33					
Smart Cover Sensor (חיישן הכיסוי החכם) 33					
הגדרות 25					
טכנולוגיה לזיהוי טביעות אצבע 35					
מאפיינים, טבלה 25					
מנעול כבל 35					
סיסמה 28					
אספקת מתח, עמידה בנחשולי מתח 35					
אספקת מתח עמידה בנחשולי מתח 35					
אתרי אינטרנט					
HP Client Automation Center 8					
HP Client Catalog עבור Microsoft SMS 10					
HP Client Management Interface 6					
HP Client Manager מ-9					
Symantec 9					
HPQFlash 15					
HP Softpaq Download Manager 6					
HP System Software Manager 7					
Proactive Change Notification 14					
Remote ROM Flash 15					
Subscriber's Choice 14					
ב					
ביטול סיסמה 31					
בקרה על גישה למחשב 25					
בקרת נכסים 25					
ג					
גישה למחשב, בקרה 25					
ד					
דיווח על שינוי 14					
דיווח על שינויים 14					
ה					
הגדרות					
העתקה למחשב אחד 17					
העתקה למספר מחשבים 18					
הגדרת לחצן הפעלה 22					
הגדרת תצורה של לחצן הפעלה 22					
הגנה על כונן קשיח 35					
הודעות כשל והתאוששות 35					
הזמנת FailSafe Key 34					
הזנה					
Power-On Password (סיסמת הפעלה) 29					
סיסמת הגדרות 29					
החלפת מערכות הפעלה, תמיכה 23					
סמלים/מספרי					
Preboot Execution) PXE (Environment) 4					

E	Emergency Recovery Mode (מצב שחזור חירום), Boot Block (בלוק אתחול) 16	HP Client Manager מ-HP	9 Symantec HP ProtectTools Security Manager 7 HP System Software Manager 7 Proactive Change (PCN) Notification 14 Remote System Installation (התקנת מערכת מרחוק) 4 Verdiem Surveyor 14 בקרת נכסים 25 טכנולוגיית ניהול 12 כלי עדכון וניהול 5 ערכת Altiris Client Management Suite 10 פריסה 2 שחזור 2 שילוב 2	נ	נעילת ה-Smart Cover Lock (מנעול הכיסוי החכם) 34
F	FailSafe Key, הזמנה 34			o	סטנדרטים מקובלים בשוק 24 סיסמה power-on 29 אבטחה 28 ביטול 31 הגדרות 28, 29 מחיקה 30 שינוי 30 סיסמת הגדרות הגדרה 28 הזנה 29 מחיקה 30 שינוי 30
H	HP			פ	פתרונות שאינם בשימוש 14
Backup and Recovery Manager	(מנהל הגיבוי והשחזור של HP) 11 Client Automation מהדורות Standard, Starter ו-Enterprise 8 Client Catalog עבור מוצרי Microsoft System Center ו- 10 SMS Client Management Interface 5			ש	שחזור, תוכנה 2 שחזור מנעול הכיסוי החכם 34 שינוי סיסמה 30
9 Symantec Client Manager	ProtectTools Security Manager 7			ת	תווי הפרדה, טבלה 31 תווי הפרדה במקלדות של שפות שונות 31 תווי הפרדה של המקלדת, שפות שונות 31 תוכנה 31
7 System Software Manager	HPQFlash 15	A	Altiris AClient 3 Client Management Suite 10 Deployment Solution Agent 3		
P	Power-On Password (סיסמת הפעלה) 29 הגדרה 29 הזנה 29 מחיקה 30 שינוי 30	B	Backup and Recovery Manager (מנהל הגיבוי והשחזור של HP) 11 BIOS Boot Block Emergency Recovery Mode (מצב שחזור חירום של בלוק אתחול) 16 HPQFlash 15 זיכרון הבזק Remote ROM Flash 15		
Preboot Execution Environment	((PXE Proactive Change (PCN) Notification) 14			C	3 Altiris AClient Altiris Deployment Solution Agent 3 Drive Protection System (מערכת להגנה על כוננים) 35 HP Backup and Recovery Manager (מנהל הגיבוי והשחזור של HP) 11 HP Client Automation מהדורות Standard, Starter ו-Enterprise 8 HP Client Catalog עבור מוצרי Microsoft System Center ו- 10 SMS HP Client Management Interface 5
7 ProtectTools Security Manager		R	Boot Block Emergency Recovery Mode (מצב שחזור חירום של בלוק אתחול) 16 Remote System Installation (התקנת מערכת מרחוק) 4	D	31 DriveLock
Boot Recovery Mode (מצב שחזור), Boot Block Emergency (מצב חירום של בלוק אתחול) 16		S			
Smart Cover FailSafe Key, הזמנה 34					

	Smart Cover Lock
34	FailSafe Key
	Smart Cover Lock (מנעול הכיסוי החכם)
34	נעילה
34	שחרור
	Smart Cover Sensor (חיישן הכיסוי החכם)
33	הגדרה
33	רמות הגנה
14	Subscriber's Choice
7	System Software Manager
	V
14	Verdiem Surveyor